

(19)日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11)特許出願公表番号
特表2001-518255
(P2001-518255A)

(43)公表日 平成13年10月9日(2001.10.9)

(51)Int.Cl. ⁷	識別記号	F I.	テリトリー (参考)
H 0 4 N 7/167		G 0 6 K 17/00	L
G 0 6 K 17/00			N
	19/00	G 0 9 C 1/00	6 6 0 A
	19/07	H 0 4 H 1/00	F
		H 0 4 N 7/167	Z
審査請求 未請求 予備審査請求 有 (全 78 頁) 最終頁に続く			

(21)出願番号 特願平10-542063
(86) (22)出願日 平成9年4月25日(1997.4.25)
(85)翻訳文提出日 平成11年9月17日(1999.9.17)
(86)国際出願番号 PCT/EP97/02107
(87)国際公開番号 WO98/43425
(87)国際公開日 平成10年10月1日(1998.10.1)
(31)優先権主張番号 97400650.4
(32)優先日 平成9年3月21日(1997.3.21)
(33)優先権主張国 ヨーロッパ特許庁 (EP)

(71)出願人 カナル プラス ソシエテ アノニム
フランス国 エフ-75711 パリ セデッ
クス 15 クアイ アンドレ シトロエン
85/89
(72)発明者 メイラード, マイケル
フランス国 エフ-28120 マインテノン
アベニュー デュ マレシャル レセル
42
(72)発明者 ベナルドゥー, クリスチアン
フランス国 エフ-77600 ビュジー サ
ン ジョルジ アレ デ ビュイザチュエ
13
(74)代理人 弁理士 斉藤 武彦 (外1名)

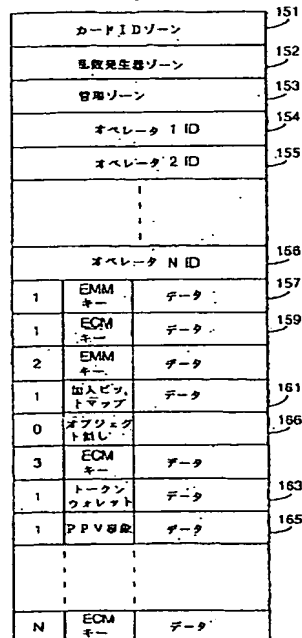
最終頁に続く

(54)【発明の名称】 暗号化放送信号の受信機と併用するためのスマートカード、および受信機

(57)【要約】

暗号化放送信号の受信機と併用するためのスマートカードは、前記信号の暗号解読を可能にするかあるいは制御するマイクロプロセッサを備えている。メモリがマイクロプロセッサに結合されている。このマイクロプロセッサは、メモリのそれぞれの動的に作成されたゾーンによってこのような信号のそれぞれの放送供給者からの複数のこのような信号の個別の暗号解読を可能にするかあるいは制御するように構成され、動的に作成されたゾーンの各々は前記放送供給者のそれぞれの放送供給者に関連した暗号解読データを記憶するように構成されている。

Fig.19.



【特許請求の範囲】

1. 暗号化放送信号の受信機と併用するためのスマートカードであって、
前記信号の暗号解読を可能にするかあるいは制御するマイクロプロセッサと、
前記マイクロプロセッサに結合されたメモリとを備え、
前記マイクロプロセッサが、前記メモリ内の各々の動的に作成されたゾーンからなる手段によってこのような信号に付いてのそれぞれの放送供給者からの複数のこのような信号の個別の暗号解読を可能にするかあるいは制御するように構成され、且つ前記動的に作成されたゾーンは各々が前記放送供給者の中のそれぞれの放送供給者に関連した暗号解読データを記憶するように構成されていることを特徴とするスマートカード。
2. 前記放送供給者の中のそれぞれの放送供給者に関連した識別子および少なくとも1つの秘密暗号解読キーをさらに備え、前記識別子および前記キーが、前記動的に作成されたゾーンの中の1つに記憶され、かつこの識別子に対応するIDを有し且つ、この暗号解読キーに対応する暗号化キーを使用して暗号化された放送信号を暗号解読するように構成され、ることを特徴とする請求項1に記載のスマートカード。
3. 各ゾーンに対して記憶されたグループ識別子と、このグループ内部のグループ識別子を識別し、前記記憶されたグループ識別子に対応するIDを有する放送信号を暗号解読するように構成された他の識別子とをさらに備えていることを特徴とする請求項2に記載のスマートカード。
4. それぞれの放送供給者のIDを含むメモリゾーンに於ける第1のシリーズ及び動的に作成されたメモリゾーンに於ける第2のシリーズとを保持するように構成され、前記第2のシリーズに於けるメモリゾーンの各々は、放送供給者のIDを示すラベルを付けられ、この供給者からの受信放送信号の処理のために使用される前記暗号解読データを含むデータ含み、第2のシリーズに於ける複数のメモリゾーンは、共通IDラベルを有し、この放送供給者からの受信放送信号の処理に関する異なる種類のデータを含むことを特徴とする前述の請求項1乃至3のいずれかに記載のスマートカード。

5. 前記スマートカードが前記第1のシリーズのメモリゾーンを動的に作成するように構成されていることを特徴とする請求項4に記載のスマートカード。

6. 前記動的に作成されたメモリゾーンが連続的であることを特徴とする前述の請求項1乃至5のいずれかに記載のスマートカード。

7. 前記動的に作成されたゾーンの動的作成を制御するデータを記憶するように構成された管理メモリゾーンをさらに備えていることを特徴とする前述の請求項1乃至6のいずれかに記載のスマートカード。

8. 一つの前記動的に作成されたゾーンが、放送供給者によって放送された放送項目の中から特定の項目を選択を示す権利データを含み、前記スマートカードの使用者暗号を解読する為の権利を有し、且つ当該スマートカードは、この供給者によって放送された項目を暗号解読するように権利データを使用する様に構成されていることを特徴とする前述の請求項1乃至7のいずれかに記載のスマートカード。

9. トランザクションメモリゾーンが、前記動的に作成されたゾーンに加えて前記スマートカードに規定され、かつ前記スマートカードのユーザが、前記ユーザの制御の下で前記スマートカードによって発生することができるトランザクション出力信号に応じてのみ暗号解読する権利が付与されている放送供給者によって放送された項目に関する他の権利データを含んでいることを特徴とするいずれかの前述の請求項に記載のスマートカード。

10. ある項目が前記トランザクション出力信号の出力に続いて放送される機会の数を計数するカウンタをさらに備え、かつ前記スマートカードが、前記カウンタによって到達された計数値に応じてこの項目の暗号解読を制御するように構成されている請求項9に記載のスマートカード。

11. 前記受信機／デコーダが、スマートカード読み取り器を備え、かつ当該スマートカード読み取り器は、前記加入者スマートカードの制御の下で放送暗号化信号を暗号解読するように構成されていることを特徴とする前述の請求項1乃至10のいずれかのに記載のスマートカードと併用するための受信機／デコーダ。

12. 前記受信機／デコーダが暗号化放送ビデオおよび／またはオーディオ信号

を暗号解読し、かつ対応するビデオおよび／またはオーディオ出力を発生するように構成されている請求項11に記載の受信機／デコーダ。

13. 前記受信機／デコーダが前記暗号化放送信号を受信する比較的高いバンド幅入力ポートと、前記出力制御信号を放送送信機に送り返すように構成された比較的低いバンド幅出力ポートとを有することを特徴とする請求項11あるいは12に記載の受信機／デコーダ。

14. 前記受信機／デコーダが、記憶された識別子を含み、かつ対応する記憶された識別子を有するスマートカードとだけ作動するように構成された請求項11～13のいずれかに記載の受信機／デコーダ。

15. 暗号化信号を受信機／デコーダに放送する装置であって、前記装置が、2又はそれ以上の種類の放送制御信号を発生する手段を備え、当該制御信号の各種類が、対応するIDを有する受信機／デコーダをこのような種類の制御信号に対して選択的に応答するようにした受信機／デコーダIDデータを含み、前記受信機／デコーダIDデータの1つあるいはそれ以上のグループの受信／デコーダの全てが、共通の種類の制御信号に応答するように構成されたグループIDデータを含み、前記装置には、入力情報に応じて異なるIDグループ間に個別の受信機／デコーダを動的に分配するように構成されているデータベース手段が装備されていることを特徴とする装置。

16. 前記データベース手段が、前記受信機／デコーダから受信された信号に応答し、グループ間の受信機／デコーダの分配を変えることを特徴とする請求項15に記載の装置。

17. 前記装置が、前記入力情報に応じてグループ間の受信機／デコーダの分配を変える制御信号を放送するように構成されたことを特徴とする請求項15あるいは請求項16に記載の装置。

18. 制御信号の異なる種類が、放送暗号化データストリームの異なる部分の暗号解読を可能にすることを特徴とする請求項15～17のいずれかに記載の装置。

19. 前記入力情報が支払い情報を含むことを特徴とする請求項15～18のいずれかに記載の装置。

20. 制御信号の当該種類が異なる放送供給者からの暗号化放送信号を暗号解読する加入操作を制御する種類を含むことを特徴とする請求項20あるいは請求項21に記載の装置。

21. 制御信号の種類が、異なる時間フレームに於ける放送暗号化データ信号を暗号解読する権利の購入を制御する種類を含むことを特徴とする請求項20あるいは請求項21に記載の装置。

22. 前記暗号化放送信号がビデオ信号および／またはオーディオ信号であることを特徴とする請求項15～21のいずれかに記載の装置。

23. 前記グループが256人までのメンバーを有することを特徴とする請求項15～22のいずれかに記載の装置。

24. 前記装置が前記暗号化データ信号を軌道を回っている衛星に送信されるように構成されていることを特徴とする請求項15～23のいずれかに記載の装置。

25. 暗号化放送信号を受信する受信機／デコーダであって、前記受信機／デコーダが、グループIDを含み、かつ前記グループIDに対応するIDを有する放送制御信号のある種類に応答し、前記受信機／デコーダが他の制御信号に応じてそのグループIDを変えるように構成されていることを特徴とする受信機／デコーダ。

26. 前記他の制御信号が放送信号を含み、前記放送信号および前記暗号化放送信号が前記受信機／デコーダによって受信されるように構成されていることを特徴とする請求項25に記載の受信機／デコーダ。

27. 前記グループIDが、前記受信機／デコーダに取り外しできるように挿入されたスマートカードに記録されていることを特徴とする請求項25あるいは26に記載の受信機／デコーダ。

28. 前記暗号化放送信号がビデオ信号および／またはオーディオ信号であることを特徴とする請求項25～27のいずれかに記載の装置。

29. 請求項25～28のいずれかに記載されるような受信機／デコーダとともに請求項15～24のいずれに記載の装置を備えているデジタルデータ信号を放送し、かつ受信するシステム。

30. 暗号化信号を受信機／デコーダに放送する方法であって、2つあるいはそ

れ以上の放送制御信号の種類を発生する工程を含み、当該信号の序番各種類は、対応するIDを有する受信機／デコーダを選択的に当該制御信号の種類に応答しうる様にするための、受信機／デコーダIDデータを含み、入力情報に応じて異なるIDグループ間に個別の受信機／デコーダを動的に分配することを含むことを特徴とする暗号化信号を受信機／デコーダに放送する方法。

31. 前記入力情報が、支払い情報を含み、且つ該制御信号の当該種類が、前記受信機／デコーダをして、暗号化放送ビデオおよび／またはオーディオストリームの一部を選択的に暗号解読せしめうるように構成したことを特徴とする請求項30に記載の方法。

32. 暗号化信号を受信機／デコーダに放送する装置であって、当該装置は、前記暗号化信号の暗号解読を制御するかあるいは可能にする制御信号を発生する手段と、制御信号を前記放送信号内部でそれぞれのプログラム伝送に関連付ける手段とを備え、前記関連付け手段が、一連の同じプログラムの伝送における各伝送を識別する信号を発生する手段を備えていることを特徴とする暗号化信号を受信機／デコーダに放送する装置。

33. 当該装置は、更に、前記受信機／デコーダに於ける、暗号解読されうる前記一連の伝送数の制限を設定する信号を発生する手段をさらに備えていることを特徴とする請求項32に記載の装置。

34. 前記装置が、受信機／デコーダからの入力信号に応じて前記制限を変更することを特徴とする請求項33に記載の装置。

35. 前記装置が、前記ビデオおよび／またはオーディオストリームを軌道を回っている衛星に送信するように構成されている請求項32～34のいずれかに記載の装置。

36. 放送信号をペイ・パー・ビュー（PPV）モードで受信し、かつ暗号解読する受信機／デコーダであって、当該受信機／デコーダは、前記放送信号内部で特定のプログラム伝送の暗号解読を可能にするかあるいは制御する制御信号を検出する手段を含み、前記制御信号が一連の同一プログラムの伝送における各伝送

を識別する情報を含むことと、前記検出手段に結合され、暗号解読されうる前記一連の伝送数を制限する手段とを備えていることを特徴とする受信機／デコーダ。

37. 前記制限手段が、前記シリーズ内の伝送の各連続視聴に応じて記憶された制限値に向けて増減されるように構成されるカウンタを備えていることを特徴とする請求項36に記載の受信機／デコーダ。

38. 受信放送信号に応じて前記制限値を調整する手段をさらに備えていることを特徴とする請求項37に記載の受信機／デコーダ。

39. 前記制限手段が、受信機／デコーダに取り外しできるように挿入されるスマートカードを備えていることを特徴とする請求項36～38のいずれかに記載の受信機／デコーダ。

40. 暗号化放送信号を受信し、かつ暗号解読する受信機／デコーダであって、
スマートカード読み取り器と、
前記スマート読み取り器に結合され、かつ前記スマートカードからの出力に応じて前記信号を暗号解読するように構成されているプロセッサと、
前記受信機／デコーダの記憶されたIDを含むメモリ手段と、
前記記憶されたIDと前記スマートカード読み取り器によって読み取られたスマートカードのIDとを比較する手段と、

前記比較に応じて前記信号の暗号解読を可能あるいは不可能にする手段とを備えていることを特徴とする受信機／デコーダ。

41. 前記可能化手段が前記スマートカードを使用可能あるいは使用禁止するように構成されている請求項40に記載の受信機／デコーダ。

42. 前記プロセッサが、前記受信機／デコーダとスマートカード間のハンドシェイクルーチンに応じて前記スマートカードを使用可能にするように構成されていることを特徴とする請求項41に記載の受信機／デコーダ。

43. 前記受信機／デコーダがビデオおよびまたはオーディオ信号を受信し、かつ暗号解読するように構成されている請求項40～42のいずれかに記載の受信機／デコーダ。

44. 前記スマートカードが、作動できるそれぞれの受信機／デコーダのIDのリストを含むメモリおよび前記スマートカードが前記リストされた受信機／デコーダの各々と作動できるかどうかについての表示を含むことを特徴とする請求項

40～43のいずれかに記載の受信機／デコーダで使用するためのスマートカード。

45. 前記受信機／デコーダが、前記スマートカードのメモリに列挙された各受信機／デコーダの前記IDを読み取る手段と、前記スマートカードが前記受信機／デコーダと同時に使用できるかどうかを決定するそれに関連した表示とを備えていることを特徴とする請求項40～43のいずれかに記載の受信機／デコーダと請求項44に記載のスマートカードとの組み合わせ。

46. 暗号化放送信号の受信機と併用するためのスマートカードであって、
前記信号の暗号解読を可能にするかあるいは制御するマイクロプロセッサと、
前記マイクロプロセッサに結合されたメモリとを備え、

前記マイクロプロセッサが、前記メモリのそれぞれのゾーンの手段によってこのような信号のそれぞれの放送供給者から複数のこのような信号の個別の暗号解読を可能にするかあるいは制御するように構成され、前記ゾーンの各々が、前記放送供給者の中のそれぞれの放送供給者に関連した暗号解読データを記憶するように構成され、前記暗号解読データが、それぞれの放送供給者によって前記スマートカードに割り当てられた優先順位レベルを含み、かつこの放送供給者によって放送されたこの優先順位レベルに関連した信号の暗号解読を可能にすることを特徴とするスマートカード。

47. 前記優先順位レベルが、前記放送供給者によって放送された制御信号によってスマートカードに割り当てられることを特徴とする請求項45に記載のスマートカード。

48. 暗号解読放送信号を受信機／デコーダに放送する装置であって、前記受信機／デコーダがそれに割り当てられたそれぞれの優先順位を有するものにおいて、前記装置が、

前記放送信号の暗号解読を制御するかあるいは可能にする制御信号を発生する

手段であって、前記制御信号の各々が、対応するアドレスを有する受信機／デコーダによる暗号解読を選択的に可能にするアドレス部を有することと、

そのそれぞれの優先順位に従って前記制御信号で受信機／デコーダを選択的に

アドレス指定する手段とを備えていることを特徴とする暗号解読放送信号を受信機／デコーダに放送する装置。

49. それぞれの放送供給者の放送信号に関連した第1のセットを構成する制御信号およびそれぞれのプログラムに関連した第2のセットを構成する制御信号を発生する手段をさらに備え、前記第2のセットの制御信号が前記受信機／デコーダによる暗号解読を制御するように構成され、前記第2のセットの制御信号が前記アドレス部を有することを特徴とする請求項48に記載の装置。

50. 前記装置が選択された地理的な位置における選択プログラムの暗号解読を中止するように構成された請求項48あるいは49に記載の装置。

51. おおむねここで添付図面に関して記載されたスマートカード。

52. おおむね添付図面の図1および図2に関して前述されたような受信機／デコーダ。

53. おおむね添付図面の図1および図2に関してここに記載されたような暗号化放送信号を受信機／デコーダに放送する装置。

54. おおむね添付図面の図1および図2に関してここに記載されたような暗号化放送信号を受信機／デコーダに放送する方法。

【発明の詳細な説明】

暗号化放送信号の受信機と併用するためのスマートカード、および受信機
産業上の利用分野

本発明は、放送・受信システムで暗号化放送信号の受信機と併用するためのスマートカード、放送信号を受信し、暗号化する受信機／デコーダ、暗号化信号を放送する装置および暗号化信号を放送する方法に関するものである。

本発明は、特に他を排斥するものではないが、下記の好ましい特徴のいくつかあるいは全てを有する大量市場放送システムに関するものである。

背景技術

この放送システムは、情報放送システム、好ましくはラジオおよび／またはテレビジョン放送システムである

(この放送システムがケーブル伝送あるいは地上伝送に応用可能し得るけれども) この放送システムは衛星システムである

この放送システムは、好ましくは、データ／信号伝送のためのMPEG、より好ましくは、MPEG-2、圧縮システムを使用するデジタルシステムである。

このシステムでは双方向の放送も可能である

この放送システムはスマートカードを使用する

用語“スマートカード”は、ここでは広義で使用され、(そのように排他的ではないが) 任意のマイクロプロセッサベースカードあるいは同様な機能および性能のオブジェクトを含んでいる。

発明の開示

第1の態様では、本発明は暗号化放送信号の受信機と併用するためのスマートカードを提供し、スマートカードは、

前記信号を使用可能するかあるいは前記信号の暗号解読を制御するマイクロプロセッサと、

前記マイクロプロセッサに結合されたメモリとを備え、

前記マイクロプロセッサが、前記メモリのそれぞれの動的に作成されたゾーン

によってこのような信号のそれぞれの放送供給者からの複数のこのような個別の暗号解読を可能にするかあるいは制御するように構成され、前記動的に作成されたゾーンの各々は、前記放送供給者の中のそれぞれの放送供給者に関連した暗号解読データを記憶するように配置されている。

スマートカードのゾーンの動的作成（および除去）は、例えば、放送局によって周期的に送信され、受信機／デコーダによって受信され、スマートカードに送られる EMM によって容易に、かつ迅速に変えられるスマートカードによって加入者に与えられた権利の為に使用される。

好ましくは、スマートカードは、前記放送供給者のそれぞれの放送供給者に関連した識別子および少なくとも 1 つの秘密暗号解読キーをさらに備え、前記識別子および前記キーあるいは各キーが、前記動的に作成されたゾーンの中の 1 つに記憶され、この識別子に対応する ID を有する放送信号を暗号解読するように構成され、この暗号解読キーに対応する暗号化キーを使用して暗号化される。

スマートカードは、各ゾーンに対して記憶されたグループ識別子と、このグループ内部のグループ識別子を識別し、記憶されたグループ識別子に対応する ID を有する放送信号を暗号解読するように構成された他の識別子とをさらに備えている。

スマートカードは、それぞれの放送供給者の ID を含むメモリゾーンからなる第 1 のシリーズおよび動的に作成されたメモリゾーンからなる第 2 のシリーズを保持するように構成されてもよく、第 2 のシリーズに於けるメモリゾーンの各々は、放送供給者の ID を示すラベルを付けられ、この供給者からの受信放送信号の処理のために使用される前記暗号解読データを含むデータを含み、第 2 のシリーズにおける複数のメモリゾーンは、共通 ID ラベルを有し、かつこの放送供給者からの受信放送信号の処理に関する異なる種類のデータを含む。

好ましくは、このスマートカードは、前記第 1 のシリーズを形成するメモリゾーンを動的に作成するように構成される。この動的に作成されたメモリゾーンは連続的であってもよい。

好ましくは、スマートカードは、前記動的に作成されたゾーンの動的作成を制御するデータを記憶するように構成された管理メモリゾーンを備えている。

前記動的に作成されたゾーンの中の1つはスマートカードのユーザが暗号解読する権利を付与される放送供給者によって放送される特定の放送項目の選択を示す権利データを含んでも良く、且つ、スマートカードは、この供給者によって放送される項目を暗号解読する前記権利データを利用するように構成されている。

トランザクションメモリゾーンは、前記動的に作成されたゾーンに加えてスマートカードに規定されてもよく、このトランザクションメモリは、ユーザの制御の下でスマートカードで生成できるトランザクション出力信号に応じてのみスマートカードのユーザが暗号解読する権利を付与される放送供給者によって放送される項目に関する他の権利データを含んでいる。

スマートカードは、項目が前記トランザクション出力信号の出力に続いて放送される機会の数を計数するカウンタをさらに備え、スマートカードは、前記カウンタによって到達される計数値に応じてこの項目の暗号解読を制御するように構成される。

本発明の第2の態様は、前述のようなスマートカードと併用するための受信機／デコーダを提供し、受信機／デコーダは、スマートカード読み取り機を備え、加入者スマートカードの制御の下で放送暗号化信号を暗号解読するように構成されている。

この受信機／デコーダは、暗号化放送ビデオおよび／またはオーディオ信号を暗号解読し、対応するオーディオおよび／またはオーディオ出力を発生させるように構成されている。

好ましくは、受信機／デコーダは、前記暗号化放送信号を受信する比較的高い帯域幅入力ポートと、出力制御信号を放送送信機に送り返すように構成された比較的低い帯域幅出力ポートとを有する。

好ましくは、受信機／デコーダは、記憶された識別子を含み、対応する記憶された識別子を有するスマートカードとだけ作動するように構成されている。

第3の態様では、本発明は、受信機／デコーダに暗号化信号を放送する装置を提供し、この装置が、2又はそれ以上の種類の放送制御信号を発生する手段を備え、当該制御信号の各種類が、対応するIDを有する受信機／デコーダをこのよ

うな種類の制御信号に対して選択的に応答するようにした受信機／デコーダIDデータを含み、前記受信機／デコーダIDデータの1つあるいはそれ以上のグループの受信／デコーダの全てが、共通の種類の制御信号に応答するように構成されたグループIDデータを含み、前記装置には、入力情報に応じて異なるIDグループ間に個別の受信機／デコーダを動的に分配するように構成されているデータベース手段が装備されている。

データベース手段は、グループ間の受信機／デコーダの分配を変えるように受信機／デコーダから受信された信号に応答してもよい。

この装置は、前記入力情報に応じてグループ間の受信機／デコーダの分配を変える放送制御信号を放送するように構成されてもよい。

異なる種類の制御信号は放送暗号化データストリームの異なる部分の暗号解読を可能にしてもよい。

好ましくは、入力情報は支払い情報を含んでいる。この種類の制御信号は、異なる放送供給者からの暗号化放送信号を暗号解読するために加入操作を制御する種類を含んでもよい。

この種類の制御信号は異なる時間フレームの放送暗号化データ信号を暗号解読する購入権を制御する種類も含んでもよい。

好ましくは、暗号化放送信号は、ビデオおよび／またはオーディオ信号であり、この装置は、前記暗号化データ信号を軌道上衛星に送信するように構成されてもよい。

各グループは256メンバーまで含んでもよい。

第4の態様では、本発明は、暗号化放送信号を受信する受信機／デコーダを提供し、受信機／デコーダは、グループIDを含み、前記グループIDに対応するIDを有するある種類の放送制御信号に応答し、受信機／デコーダは、他の制御信号に応じてそのグループIDを変えるように構成されている。

他の制御信号は放送信号を含み、前記放送信号および前記暗号化放送信号は前記受信機／デコーダによって受信されるように構成されている。

好ましくは、グループIDは、受信機／デコーダに取り外しできるように挿入されるスマートカードに記録される。前記暗号化放送信号はビデオおよび／また

はオーディオ信号でもよい。

第5の態様では、本発明は、前述のように受信機／デコーダとともに前述のような装置を含むデジタルデータ信号を放送し、受信するシステムを提供する。

第6の態様では、本発明は、暗号化信号を受信機／デコーダに放送する方法を提供し、この方法は、2つあるいはそれ以上の放送制御信号の種類を発生する工程を含み、当該信号の序番各種類は、対応するIDを有する受信機／デコーダを選択的に当該制御信号の種類に応答しうる様にするための、受信機／デコーダIDデータを含み、入力情報に応じて異なるIDグループ間に個別の受信機／デコーダを動的に分配する。

入力情報は、好ましくは、支払い情報を含み、且つ前記受信機／デコーダをして、暗号化放送ビデオおよび／またはオーディオストリームの一部を選択的に暗号解読せしめうる制御信号を更に含んでいる。

第7の態様では、本発明は、暗号化信号を受信機／デコーダに放送する装置を提供し、この装置は、前記暗号化信号の暗号解読を制御するかあるいは可能にする制御信号を発生する手段と、制御信号を前記放送信号内部でそれぞれのプログラム伝送と関連付ける手段とを備え、関連付ける手段は、一連の同じプログラム伝送において各伝送を識別する信号を発生する手段を備えている。

好ましくは、この装置は、暗号解読できる前記一連の伝送数に対する制限を受信機／デコーダに設定する信号を発生する手段をさらに備えている。この装置は、前記制限を変えるように受信機／デコーダからの入力信号に応答してもよい。

好ましくは、この装置は、前記ビデオおよび／またはオーディオストリームを軌道上衛星に送信するように構成されている。

第8の態様において、本発明は、放送信号をペイ・パー・ビュー（PPV）モードで受信し、かつ暗号解読する受信機／デコーダを提供し、当該受信機／デコーダは、前記放送信号内部で特定のプログラム伝送の暗号解読を可能にするかあるいは制御する制御信号を検出する手段を含み、前記制御信号が一連の同一プログラムの伝送における各伝送を識別する情報を含むことと、前記検出手段に結合され、暗号解読されうる前記一連の伝送数を制限する制限手段とを備えている。

好ましくは、制限手段は、前記シリーズ内の伝送の各連続視聴に応じて記憶された制限値に向けて増減されるように構成されるカウンタを備えている。

又、当該制限手段は、受信放送信号に応じて前記制限値を調整する手段をさらに備えている。

好ましくは、制限手段は、前記一連内部の伝送の各連続視聴に応じて記憶された制限値の方へ増減されるように構成されたカウンタを備えている。受信機／デコーダは、好ましくは、受信放送信号に応じて前記制限値を調整する手段を備えている。

好ましくは、制限手段は、受信機／デコーダに取り外しできるように挿入されたスマートカードを備えている。

第9の態様において、本発明は、暗号化放送信号を受信し、暗号解読する受信機／デコーダを提供し、この受信機／デコーダは、

スマートカードと、

スマートカードに結合され、かつスマートカードからの出力に応じて前記信号を暗号解読するように構成されているプロセッサと、

受信機／デコーダの記憶IDを含むメモリ手段と、

前記記憶されたIDとスマートカード読み取り器によって読み取られたスマートカードのIDとを比較する手段と、

比較に応じて前記信号の暗号解読を可能にするかあるいは不可能にする手段とを備えている。

可能化手段は前記スマートカードを使用可能あるいは使用禁止にするように構成されてもよい。

プロセッサは、受信機／デコーダとスマートカードとの間のハンドシェークに応じて前記スマートカードを使用可能にするように構成されてもよい。

受信機／デコーダは、放送ビデオおよび／またはオーディオ信号を受信し、暗号解読するように構成されてもよい。

第10の態様において、本発明は、前述のように受信機／デコーダで使用するためのスマートカードを提供し、前記スマートカードは、スマートカードが操作

できるそれぞれの受信機／デコーダのIDのリストを含むメモリと、スマートカードが前記リストされた受信機／デコーダの各々で操作できるかどうかに関する表示とを含む。

第11の態様において、本発明は、前述のような受信機／デコーダと前述のようなスマートガードとの組み合わせを提供し、前記受信機／デコーダは、前記スマートカードのメモリにリストされた各受信機／デコーダのIDを読み取る手段と、スマートカードが受信機／デコーダと併用されてもよいかどうかを決定するそれに関連した表示とをさらに備えている。

第12の態様において、本発明は、暗号化放送信号の受信機と併用するためのスマートカードを提供し、このスマートカードは、

前記信号の暗号解読を可能にするかあるいは制御するマイクロプロセッサと、
前記マイクロプロセッサに結合されたメモリとを備え、

前記マイクロプロセッサは、前記メモリのそれぞれのゾーンによってこのような信号のそれぞれの放送供給者からの複数のこのような信号の個別の暗号解読を可能にするかあるいは制御するように構成され、前記ゾーンの各々が前記放送供給者の中のそれぞれの放送供給者に関連した暗号解読データを記憶するように構成され、前記暗号解読データは、それぞれの放送供給者によってスマートカードに割り当てられた優先順位レベルを含み、この放送供給者によって放送された優先順位レベルに関連した信号の暗号解読を可能にする。

この優先順位のレベルは、放送供給者によって放送された制御信号によってスマートカードに割り当てられてもよい。

第13の態様において、本発明は、暗号化放送信号を受信機／デコーダに放送する装置を提供し、前記受信機／デコーダはそれに割り当てられたそれぞれの優先順位を有し、この装置は、

前記放送信号の暗号解読を制御するかあるいは可能にする制御信号を発生する手段であって、前記制御信号の各々は対応するアドレスを有する受信機／デコーダによって暗号解読を選択的に可能にするアドレス部を有することと、

そのそれぞれの優先順位レベルに従って前記制御信号で受信機／デコーダを選

択的にアドレス指定する手段とを備えている。

この装置は、放送信号のそれぞれの放送供給者に関連した第1のセットを構成する制御信号およびそれぞれに関連した第2のセットを構成する制御信号を発生する手段をさらに備えてもよく、第2のセットにおける制御信号が受信機／デコーダによる暗号解読をゲートで制御するように構成されたスイッチング部を有し、前記第2のセットの制御信号は前記アドレス部を有する。

この装置は選択された地理的な位置で選択されたプログラムの暗号解読を停止するように構成されてもよい。

図面の簡単な説明

図1は、本発明の好ましい実施例によるデジタルテレビジョンシステムの全アーキテクチャを示している。

図2は、デジタルテレビジョンシステムの条件付アクセスシステムのアーキテクチャを示している。

図3は、条件付アクセスシステムで使用された権利付与管理メッセージの構造を示している。

図4は、本発明の好ましい実施例による加入者許可システム（SAS）のハードウェアの概略図である。

図5は、SASのアーキテクチャの概略図である。

図6は、SASの一部を形成する加入者技術管理サーバの概略図である。

図7は、SASによって実行されるような加入の自動更新のための手順の流れ図である。

図8は、自動更新手順で使用されたグループ加入ビットマップの概略図である。

図9は、自動更新手順で使用されたEMMの構造を示している。

図10は、EMMの構造を詳細に示している。

図11は、通信サーバを通して直接コマンドを受信するために使用される場合の注文集中化サーバの概略図である。

図12は、本発明の一実施例を示す図2の一部を概略的に示している。

図13は、コールバックをリクエストするように加入者許可システムからのコ

マンドを受信するために使用される場合の注文集中化サーバの概略図である。

図14は、通信サーバの概略図である。

図15は、EMM放出サイクル速度がPPVイベントのタイミングにより変更される方法を示している。

図16は、EMMを放出するために使用されるメッセージ放出器の概略図である。

図17は、メッセージ放出器内部のEMMの記憶の方法を示す概略図である。

図18は、スマートカードの概略図である。

図19は、スマートカードのメモリゾーンの配置の概略図である。

図20は、PPVイベント説明の概略図である。

発明を実施する為の最良の態様

本発明の好ましい特徴は、次に単に例として添付図面を参照して述べられる。

本発明によるデジタルテレビジョン放送・受信システム1000の概略が図1に示されている。本発明は、圧縮デジタル信号を送信するために既知のMP EG-2を使用する主に従来のデジタルテレビジョンシステム2000を含んでいる。より詳細には、放送センターのMP EG-2圧縮器2002は、デジタル信号ストリーム（一般的にはビデオ信号のストリーム）を受信する。この圧縮器2002は、リンケージ2006によってマルチプレクサ・スクランブラ2004に接続されている。マルチプレクサ2004は、複数の他の入力信号を受信し、1つあるいはそれ以上のトランスポートストリームを組み立て、テレコムリンクを含む様々な形式をとることができるリンケージ2010を介して放送センターの送信機2008に圧縮デジタル信号を送信する。送信機2008は、電磁信号が電子的に処理され、従来はエンドユーザによって所有されるかあるいは賃貸された皿形の地上受信機2018に概念的なダウンリンク2016を介して放送する。受信機2018によって受信された信号は、エンドユーザによって所有されるかあるいは賃貸された複合受信機／デコーダ2020に送信され、エンドユーザのテレビジョンセット2022に接続されている。この受信機／デコーダ2020は、圧縮MP EG-2信号をテレビジョンセット2022のための

テレビジョン信号に復号化する。

条件付アクセスシステム3000は、マルチプレクサ2004および受信機／デコーダ2020に接続され、一部は放送センターに、一部はデコーダに置かれている。条件付アクセスシステム3000は、エンドユーザが1つあるいはそれ以上の放送供給者からのデジタルテレビジョン放送にアクセスすることを可能にする。商業オファー（すなわち、放送供給者によって販売された1つあるいはいくつかのテレビジョンプログラム）に関するメッセージを解読できるスマートカードは受信機／デコーダ2020に挿入できる。デコーダ2020およびスマートカードを使用して、エンドユーザは、加入モードあるいはペイ・パー・ビューモードのいずれかのイベントを購入できる。

マルチプレクサ2004および受信機／デコーダ2020にも接続され、さらに一部は放送センターに置かれ、一部はデコーダに置かれている対話式システム4000によって、エンドユーザはモデムバックチャネル4002を介して様々なアプリケーションと対話できる。

条件付アクセスシステム3000は、次により詳細に述べられる。

図2を参照するに、概略において、条件付アクセスシステム3000は、加入者許可システム（SAS）3002を含んでいる。SAS3002は、それぞれのTCP-IPリンケージ3006（その代わりに他のリンケージのタイプが使用できるけれども）によって1つあるいはそれ以上の加入者管理システム（SMS）3004に接続される。1つのSMSは各々の放送供給者に対するものである。その代わりに、1つのSMSは2つの放送供給者間に共有することができるか、あるいは1つの供給者は2つのSMS等を使用できる。

「マザー」スマートカードを利用する暗号化装置3008の形の第1の暗号化装置は、リンケージ3012によってSASに接続されている。また、マザースマートカード3016を利用する暗号化装置3014の形の第2の暗号化装置はリンケージ3018によってマルチプレクサ2004に接続されている。受信機／デコーダ2020は「ドーター」スマートカード3020を受け取る。受信機／デコーダ2020は、モデムバックチャネル4002を介して通信サーバ30

22によってSAS3002に直接接続される。SASは、要求に応じてドータースマートカードに加入権を送信する。

このスマートカードは1つあるいはそれ以上の商業オペレータの秘密を含む。

「マザー」スマートカードは異なる種類のメッセージを暗号化し、「ドーター」スマートカードは、このスマートカードがメッセージを解読する権利を有するならば、メッセージを解読する。

第1および第2の暗号化装置3008および3014は、ラックと、EEPROM上に記憶されたソフトウェアを有するVMEカードと、20枚までの電子カードおよび各電子カードに対してそれぞれECMを暗号化するカード（カード3016）と、EMMを暗号化するカード（カード3010）の1枚のスマートカード3010および3016とを含む。

デジタルテレビジョンシステムの条件付アクセスシステム3000の動作は、次にテレビジョンシステム2000および条件付アクセスシステム3000の様々な構成要素を参照してより詳細に述べられる。

マルチプレクサ・スクランブラ

図1および図2に参照すると、放送センターにおいて、デジタルビデオ信号は、MPEG-2圧縮器2002を使用して、最初に圧縮される（あるいはビットレート減少される）。この圧縮信号は、次に他の圧縮データのような他のデータで多重化されるためにリンケージ2006を介してマルチプレクサ・スクランブラ2004に伝送される。

このスクランブラは、スクランブル処理で使用され、マルチプレクサ2004においてMPEG-2ストリームに含まれた制御語を生成する。この制御語は、内部で生成され、ユーザの統合受信機／デコーダ2020がプログラムを暗号解読することを可能にする。

いかにプログラムが商品化されるかを示すアクセス基準はMPEG-2ストリームにも付加される。このプログラムは、多数の「加入」モードの中の1つおよび／または多数の「ペイ・パー・ビュー」（PPV）モードあるいはイベントの中の1つのいずれかで商品化されてもよい。

加入モードでは、エンドユーザは、1つあるいはそれ以上の商業オファー、すなわち「ブーケ」(bouquet)を申し込むので、これらのブーケ内部のあらゆるチャンネルを見る権利を得る。

好ましい実施例では、960までの商業オファーはチャンネルのブーケから選択されてもよい。ペイ・ビュー・ビューモードでは、エンドユーザには、望むようなイベントを購入する機能が提供される。これは、イベントを前もってプレブックすることあるいはイベントが放送されるや否や購入することのいずれかによって行うことができる。好ましい実施例では、全てのユーザが加入モードあるいはPPVモードで見ても見なくても、全てのユーザは加入者であるが、もちろん、PPV視聴者は必ずしも加入者である必要がない。

制御語およびアクセス基準の両方は、権利付与制御メッセージ(ECM)を形成するために使用される。すなわちこれは1つのスクランブルプログラムとの関連で送信されるメッセージである。すなわちこのメッセージは、放送プログラムの(プログラムのデスクランブルを可能にする)制御語およびアクセス基準を含む。アクセス基準および制御語は、リンケージ3018を介して第2の暗号化装置3014に伝送される。この装置では、ECMは生成され、暗号化され、マルチプレクサ・スクランブラ2004上に伝送される。

データストリームにおける放送供給者によって放送される各サービスは多数の別個の構成要素を含んでいる。すなわち、例えば、テレビジョンプログラムは、ビデオ構成要素、オーディオ構成要素、サブタイトル構成要素等を含んでいる。サービスのこれらの構成要素の各々は、トランスポンダ2014にその後に放送するために個別にスクランブルされ、暗号化される。サービスの各スクランブルされた構成要素に関しては、別個のECMが要求される。

プログラム送信

マルチプレクサ2004は、SAS3002からの暗号化EMMと、第2の暗号化装置3014からの暗号化ECMと圧縮器2002からの圧縮プログラムとを含む電気信号を受信する。マルチプレクサ2004は、プログラムをスクランブルし、スクランブルされたプログラム、暗号化EMMおよび暗号化ECMを電

気信号として放送センターの送信機2008にリンケージ2010を介して送信する。送信機2008は、アップリンク2012を介して衛星トランスポンダ2014の方へ電磁信号を送信する。

プログラム受信

衛星トランスポンダ2014は、送信機2008によって送信された電磁信号を受信し、処理し、ダウンリンク2016を介して、従来はエンドユーザによって所有されるかあるいは賃貸された皿形の地上受信機2018上に送信する。受信機2018によって受信された信号は、エンドユーザによって所有されるかあるいは賃貸された統合受信機／デコーダ2020に送信され、エンドユーザのテレビジョンセット2022に接続される。この受信機／デコーダ2020は、暗号化ECMおよび暗号化ECMを有するスクランブルされたプログラムを得るために信号を多重分離する。

プログラムがスクランブルされない場合、すなわち、ECMがMPEG-2ストリームとともに全く送信されない場合、受信機／デコーダ2020は、データを分解し、この信号をテレビジョンセット2022に送信するためのビデオ信号に変換する。

プログラムがスクランブルされる場合、受信機／デコーダ2020は、対応するECMをMPEG-2ストリームから抽出し、ECMをエンドユーザの「ドーター」スマートカード3020に送る。これは、受信機／デコーダ2020のハウジングにうまくはまる。ドータースマートカード3020は、エンドユーザがECMを暗号解読し、プログラムにアクセスする権利を有するかどうかを制御する。有していない場合、負の状態は、受信機／デコーダ2020に送られ、プログラムが暗号解読できないことを示す。エンドユーザが権利を有する場合、ECMは暗号解読され、制御語が抽出される。次に、デコーダ2020は、この制御語を使用してプログラムを暗号解読できる。MPEG-2ストリームは、伸長され、テレビジョンセット2022に前方送信するためのビデオ信号に変換される。

加入者管理システム (SMS)

加入者管理システム（SMS）3004は、特にエンドユーザファイル、商業オファー（例えば、料金およびプロモーション）、加入、PPV詳細、エンドユーザ消費および許可に関するデータの全てを管理するデータベース3024を含んでいる。SMSは、物理的にSASから遠隔であってもよい。

各SMS3004は、エンドユーザに送信される権利付与管理メッセージ（EMM）の変更あるいは形成を意味するメッセージをそれぞれのリンケージ3006を介してSAS3002に送信する。

SMS3004は、EMMの変更およびEMMの形成を意味せず、（製品を注文する場合、エンドユーザに付与された許可あるいはエンドユーザが請求される額に関する）エンドユーザの状態の変化のみを意味するメッセージをSAS3002にも送信する。

後述されるように、SAS3002は、（一般的にはコールバック情報あるいは課金情報のような情報を要求する）メッセージをSMS3004に送信するので、2つの間の通信が双方向であることは明らかである。

エンタイトルメントマネジメントメッセージ（EMM）

EMMは、（1つのスクランブルされたプログラムだけ、あるいは同じ商業オファーの一部である場合にはスクランブルされたプログラムのセットに専用であるECMと対比して）個人エンドユーザ（加入者）、あるいはエンドユーザのグループに専用のメッセージである。各グループには所定数のエンドユーザが含まれる。

グループとしてのこの構成はバンド幅を最適化することを目指している。

すなわち、1つのグループへのアクセスは多数のエンドユーザへの到達を可能にできる。

様々な特定のタイプのEMMは、本発明を実施する際に使用される。個人EMMは個人加入者に専用であり、一般的にはペイ・パー・ビューサービスと共に使用される。

すなわち、これらは、このグループのグループ識別子および加入者の位置を含む。いわゆる「グループ」加入EMMは、例えば、256人の個人ユーザのグル

ープに専用であり、一般的にはいくつかの加入サービスの管理に使用される。

EMMは、グループ識別子および加入者のグループビットマップを有する。聴衆EMMは、全聴衆に専用であり、例えば、ある種の無料サービスを提供するために特定のオペレータによって使用されてもよい。

「聴衆」は、同じオペレータ識別子（OPI）を搭載するスマートカードを有する全体の加入者である。最後に、「ユニーク」EMMはスマートカードのユニーク識別子に向けられる。典型的なEMMの構造は、次に図3を参照して述べられる。基本的には、一連のデジタルデータビットとして実現されるEMMは、

ヘッダ3060と、ユニークEMM3062と、シグネチャ3064とを含む。次に、ヘッダ3060は、タイプが個人、グループ、聴衆あるいは若干の他のタイプであるかどうかを識別するタイプ識別子3066と、EMMの長さを示す長さ識別子3068と、EMMのための任意のアドレス3070と、オペレータ識別子3072と、キー識別子3074とを含む。ユニークEMM3062は、もちろんそのタイプに従って大いに変わる。最後に、一般的には8バイトの長さであるシグネチャ3064は、EMMの残りのデータの破損に対して多数のチェックを行う。

加入者許可システム（SAS）

SMS3004によって生成されたメッセージは、リンケージ3006を介して加入者許可システム（SAS）3002に送られ、この加入者許可システム（SAS）3002は、次にSMS3004によって生成されたメッセージの受信を肯定応答するメッセージを生成し、これらの肯定応答をSMS3004に送る。

図4に示されるように、ハードウェアレベルで、SASは、既知の方法で、データおよびコマンド入力のための1つあるいはそれ以上のキーボード3052に接続されたメインフレームコンピュータ3050（好ましい実施例では、DECマシン）と、出力情報の表示のための1つあるいはそれ以上の表示装置（VDU）3054と、データ記憶手段3056とを備えている。ハードウェアにある程度の冗長性が与えられてもよい。

ソフトウェアレベルで、SASは、好ましい実施例では、標準オープンVMSオペレーティングシステム、すなわちそのアーキテクチャが次に図5を参照して概説で述べられる一連のソフトウェアで実行する。すなわち、ソフトウェアがその代わりにハードウェアで実現できることが理解される。

概説において、SASは、加入モードのための権利を与え、毎月この権利を自動的に更新する加入チェーン領域3100と、PPVイベントのための権利を与えるペイ・パー・ビューチェーン領域3200と、加入・PPVチェーン領域によって形成されたEMMをマルチプレクサ・スクランブラ2004に送るので、EMMを有するMPEGストリームを供給するEMMインジェクタ3300とを備えている。

ユーザのパーソナルコンピュータにコンピュータソフトウェアをダウンロードする場合のペイ・パー・ファイル(PPF)権利のような他の権利が付与されるべきである場合、他の同様な領域も装備される。

SAS3002の1つの機能は、加入モードで商業オファーとして利用されるかあるいは異なる商品化のモード(プレブックモード、インパルスモード)によるPPVイベントとして販売されるテレビジョンプログラムへのアクセス権を管理することにある。これらの権利およびSMS3004から受信された情報により、SAS3002は、加入者のためのEMMを生成する。

加入チェーン領域3100は、コマンドインタフェース(CI)3102と、加入者技術管理(STM)サーバ3104と、メッセージ生成器(MG)3106と、暗号化装置3008とを備えている。PPVチェーン領域3200は、許可サーバ(AS)3202と、エンドユーザの関連詳細を記憶するリレーショナルデータベース3204と、データベースのためのローカルブラックリストデータベース3205と、データベースのためのデータベースサーバ3206と、注文集中化サーバ(OC S)3207と、プログラム放送器のためのサーバ(SP B)3208と、その機能が加入チェーン領域のための機能と基本的に同じであるので、さらに少しも詳述されないメッセージ生成器(MG)3210と、暗号化装置3008とを備えている。

EMMインジェクタ3300は、複数のメッセージ放出器3302、3304、3306および3308およびソフトウェアマルチプレクサ(SMUX)3310および3312を備えている。好ましい実施例では、メッセージ生成器3210のための他の2つのME3306および3308とともにメッセージ生成器3106のための2つのME3302および3304がある。ME3302および3306は、SMUX3310に接続されるのに対して、ME3304および3308はSMUX3312に接続される。

SASの3つの主要構成要素(加入チェーン領域、PPVチェーン領域およびEMMインジェクタ)の各々は、次により詳細に考察される。

加入チェーン領域

最初に加入チェーン領域3100を考察すると、コマンドインタフェース3102は、主にSMS3004からSTMサーバ3104ならびにOCS3206に、およびOCSからSMSにメッセージを急送するためのものである。コマンドインタフェースは、SMSからの入力として直接コマンドあるいはコマンドを含むバッチファイルをとる。コマンドインタフェースは、STMサーバからくるメッセージで構文分析を実行し、エラーがメッセージで生じる場合、正確なメッセージを放出できる(範囲外のパラメータ、見つからないパラメータ等)。コマンドインタフェースは、一連のコマンドを再生できるようにトレースファイル3110におけるテキスト形式の入力コマンドおよび再生ファイル3112における2進形式の入力コマンドもトレースする。トレースは使用禁止され、ファイルのサイズは制限される。

STMサーバ3104の詳細は、次に特に図6を参照して述べられる。効果的にはSTMサーバは加入チェーン領域の主エンジンであり、無料権利を管理する目的、新規の加入者の作成、および現在の加入者の更新を有する。

図で示されるように、コマンドは、コマンドがSTMサーバに送られるフォーマットとは異なるフォーマットであるが、メッセージ生成器3106に渡される。

各コマンドに関しては、STMサーバは、関連コマンドが効果的に処理され、

MGに送られる場合だけ肯定応答メッセージをCIに送信するように構成されている。

STMは、加入者の全ての関連パラメータ（スマートカード番号、商業オファ—、状態、グループおよびグループの位置等）が記憶される加入者データベース3120を含む。このデータベースは、データベースの内容に対してCI3102によって送信されたコマンドの意味チェックを実行し、コマンドが有効である場合、データベースを更新する。

STMサーバは、STMサーバとMGとの間のファーストインファーストアウト（FIFO）バッファ3122ならびにバックアップディスクFIFO3124をさらに管理する。FIFOの目的は、MGが任意の理由のためにしばらく応答できない場合、CIからのコマンドの流れを平均化することにある。FIFOは、再開始される場合、STMサーバはそのFIFOを空にする（すなわち、M

Gに送信する）ように構成されているので、STMサーバあるいはMGがクラッシュした場合、コマンドが全く失われないことも確実にすることができる。FIFOはファイルとして実現される。

STMサーバは、更新およびオペレータによって要求されるならば、無料権利を自動的に生成する自動更新サーバ3126をその中心部に含む。これに関連して、新規の権利の生成がSMSで開始されることが理解されるけれども、更新の生成は、初めて権利の生成を含むものとみなすことができる。明らかになるように、2つはおよそ同じコマンドおよびEMMによって処理できる。

重要な機能は、SMSからSASに送られることが必要であるコマンドの数を著しく減らすことができるので（SMSおよびSASが異なる位置にあり、異なるオペレータによって操作されてもよいことを覚えておく）、SASから離れたSTMおよびSMS3004において（既知システムにおいて）よりもむしろSAS内部の自動更新サーバを有することは特に重要な機能である。

実際、SMSから要求された2つの主コマンドは、新規の加入が開始されるべきであり、現在の加入が停止されるべき（例えば、未払いの場合）である単なるコマンドである。SMSとSASとの間のコマンド交換を最少にすることによっ

て、2つの間のリンケージ3006におけるコマンド転送の障害の可能性が減少される。さらに、SMSの設計は、条件付アクセスシステム3000の機能を一般に考慮する必要がない。

自動更新は図7の流れ図に示されたように進行する。バンド幅を減らすために、全更新の中の非常に高いパーセンテージが標準である場合、更新は加入者のグループにおいて進行する。

すなわち、好ましい実施例では、グループ毎に256人の個人加入者がある。流れ図は、開始ステップ3130で開始し、毎月の更新機能の作動が行われるステップ3132に進む（もちろん、他の回数でも可能であることが理解されるけれども）。毎月の頻度で、権利は、エンドユーザに現在の月および次の月の全ての間に与えられ、その時点で権利が、更新されない場合は、終了する。

ステップ3134で、加入者データベース3120は、特定の個人のための権利が更新されるべきであるかどうかを決定するために各グループおよびこのグル

ープ内部の各個人に関してアクセスされる。

ステップ3136で、グループ加入ビットマップは、図8に示されるように加入者データベースの内容により設定される。このビットマップは、グループ識別子（この場合、グループ1 - 「G1」）3138および256の個人加入者ゾーン3140を含んでいる。ビットマップの個別のビットは、特定の加入者が更新される権利を有するべきであるか否かにより1あるいは0にセットされる。典型的な2進データのセットはこの図に示されている。

ステップ3142で、グループ加入ビットマップを含む適当なコマンドは、メッセージ生成器3106に送られる。ステップ3143で、メッセージ生成器は、特定の加入EMMが有効でない日付をスマートカードを表示するように陳腐化日付を設定する。すなわち、一般的には、この日付は、次の月の末日として設定される。

ステップ3144で、メッセージ生成器は、コマンドから適当なグループ加入EMMを発生し、暗号化装置3008にEMMを暗号化するように求め、それから、暗号化EMMは、ステップ3146で、EMMをMPEG-2データストリ

ームに入れるEMMインジェクタ3300に送られる。

ステップ3148は、前述の手順が各グループおよび毎グループに対して繰り返されることを示している。

実際、図7を参照して前述された流れ図は、特に加入の更新に関するものである。STMも同様に無料聴衆権利および新規加入者を管理する。

特定のテレビジョンプログラムあるいはこのようなプログラムのグループに役に立つ無料聴衆権利の場合、これらは、コマンドをメッセージ生成器に出し、所与の日数（あるいは週数）の陳腐化日付を有する適当な聴衆EMM（全聴衆に対して）を発生するSTMによって利用される。MGは、STMコマンドに基づいて正確な陳腐化日付を計算する。

新規加入者の場合、これらは2つの工程で処理される。まず第一に、買物の際に、受信機／デコーダ2020におけるスマートカード（所望ならば、オペレータによって）は、所与の期間（一般的には2、3日）加入者無料権を与える。これは、関連陳腐化日付を含む加入者のためのビットマップを生成することによって実行される。

次に、加入者は、完了された事務手続きを、加入者を（SMSで）管理するオペレータに渡す。一旦事務手続きが処理されると、SMSは、この特定の加入者のための開始コマンドをSASに供給する。開始コマンドのSASによる受信の際、STMは、MGに命令し、ユニークアドレスを新規加入者（特定のグループ番号およびグループ内部の位置を有する）に割り当て、（更新のために使用されたより普通の「グループ」加入EMMとは対照的に）特別のいわゆる「商業オフアー」加入EMMを生成し、次の月の月末まで、特定の加入者に権利を与える。

この時点から、加入者の更新は前述のように自動的に生じ得る。この2つの工程処理によって、SMSが停止コマンドを発するまで、新規加入者権利を付与することができる。

商業オフアー加入EMMが新規加入者および現在の加入者の再アクティベーションのために使用されることに注目すべきである。グループ加入EMMは更新目的および停止目的のために使用される。

図9を参照すると、前述の手順によって生成された典型的なユニーク加入EMM（すなわち、ヘッダおよびシグネチャを無視する）は、下記の主要な部分、すなわち、一般的には256ビットの加入（あるいは加入者のグループ）ビットマップ3152と、EMMの暗号化のための128ビットの管理暗号化キー3154と、放送プログラムにアクセスするためにスマートカード3020が制御語を暗号解読できる64ビットの各利用暗号化キー3156と、スマートカードがEMMを無視する日付を表示する16ビットの陳腐化日付3158とを含んでいる。

実際、好ましい実施例では、3つの利用キーが備えられ、1つのキーが今月のためにセットされ、1つのキーが来月のためにセットされ、1つのキーがシステム障害の場合の再開目的のためのものである。

より詳細には、グループ加入ユニークEMMは、管理暗号化キー3154を除いて上記の構成要素の全てを有する。商業オファ加入ユニークEMM（個人加入者のためのものである）は、全加入者のグループビットマップ3152の代わりにグループにおける位置が続くグループIDを含み、それから関連陳腐化日付

3158が続く管理暗号化キー3154および3つの利用キー3156を含んでいる。

メッセージ生成器3106は、STMサーバによって発されたコマンドをメッセージ放出器3302に送るためのEMMに変換するのに役立つ。図5を参照すると、まず第一に、MGは、ユニークEMMを発生し、これを管理キーおよび利用キーに関して暗号化する暗号化装置3008に送る。CUは、EMMのシグネチャ3064（図3を参照）を完了し、EMMをヘッダ3060が付加されるMGに返送する。したがって、メッセージ放出器に送られたEMMは全EMMである。メッセージ生成器も、放送開始・中止時間およびEMMの放出速度を決定し、これらをEMMとともに適当な指令としてメッセージ放出器に送る。MGだけが所与のEMMを1回発生する。すなわち、それは周期的送信を実行するMEである。

再度、図5を参照すると、メッセージ生成器は、関連EMMの存続期間、それ

を記憶するそれ自体のEMMデータベース3160を含む。一旦その放出持続期間が満了すると、関連EMMが削除される。データベースは、MGとMEとの間の整合性を確実にするために使用されるので、例えば、エンドユーザが資格を一時的に取り上げられる場合、MEは更新を送信し続けない。この点では、MGは関連演算を計算し、これをMEに送信する。

EMMの生成の際に、MGはユニーク識別子をEMMに割り当てる。MGはEMMをMEに送る場合、MGもEMM IDを送る。これは、MGおよびMEの両方で特定のEMMの識別を可能にする。

さらに、加入チェーン領域に関しては、メッセージ生成器は、暗号化EMMを記憶する2つのFIFO3162および3164を含み、このFIFOはEMMインジェクタ3300における関連メッセージ放出器3302および3304の各々のためのものである。加入チェーン領域およびEMMインジェクタは、かなりの距離を隔てて離れてもよいので、たとえ2つの間のリンク3166および3168が故障するとしても、FIFOの使用はEMM送信において完全な連続性を可能にすることができる。同様なFIFOはペイ・パー・ビューチェーン領域に備えられる。

特にメッセージ発生器および一般に条件付アクセスシステムの1つの特定の機能は、空間を節約するパラメータ長および識別子を混合することによってユニークEMM3062の長さを減少する方法に関するものである。これは、次に、典型的なEMM（実際、最も簡単なEMMであるPPV EMM）を示す図10を参照して述べられる。長さの減少は、Pid（パケットあるいは「パラメータ」識別子）3170で生じる。

これは、2つの部分、すなわち実際のID3172およびパケットのための長さパラメータ3174（次のパケットの開始が識別することができるために必要である）を含む。全Pidは、ちょうど1バイトの情報で示される。すなわち、4ビットはIDのために用意され、4ビットが長さのために用意される。4ビットは真の2進法で長さを規定するには十分でないので、ビットと実際の長さとの間の異なる相応関係が使用され、この相応関係は、メッセージ生成器における記

憶領域3178に記憶されたルックアップテーブルに示されている（図5を参照）。相応関係は、一般的には下記の通りである。

0000 = 0

0001 = 1

0010 = 2

0011 = 3

0100 = 4

0101 = 5

0110 = 6

0111 = 7

1000 = 8

1001 = 9

1010 = 10

1011 = 11

1100 = 12

1101 = 16

1110 = 24

1111 = 32

長さパラメータはパケットの実際の長さに正比例していないことが分かる。この関係は部分的には線形よりもむしろより方形のようである。これにより、より大きな範囲のパケットの長さが提供される。

ペイ・パー・ビューチェーン領域

ペイ・パー・ビューチェーン領域3200に関しては、図5をより詳細に参照すると、許可サーバ3202は、PPV製品を購入するために通信サーバ3022に接続する各加入者についての情報を要求する注文集中化サーバ3207をそのクライアントとして有する。

加入者がAS3202から識別されるならば、トランザクションのセットが行われる。加入者が注文を許可された場合、ASは請求書を作成し、それをOCS

に送る。さもなければ、A Sは注文が許可されないという信号をO C Sに送出する。

少なくとも1つのトランザクションが許可された場合、A Sがデータベースサーバ(D B A S) 3 2 0 6を介してエンドユーザデータベース3 2 0 4を更新することは、このトランザクションのセットの終了時だけである。これにより、データベースアクセス数が最適化される。

A Sが購入を許可する基準は、D B A S処理を通してアクセスされるデータベースに記憶される。1つの実施例では、データベースはS T Mによってアクセスされるデータベースと同じである。

消費者プロフィールに応じて、許可は否定されてもよい(P P V__F o r b i d d e n, C a s i n o__F o r b i d d e n. . .)。これらの種類の基準は、S M S 3 0 0 4のためにS T M 3 1 0 4によって更新される。

購入のために許可された限界などを(クレジットカード、自動支払い、1日あたりの許可トークン購入数のいずれかによる)他のパラメータがチェックされる。

クレジットカードで支払いの場合、カードの番号は、ローカルブラックリストデータベース3 2 0 5に記憶されたローカルブラックリストを基準にしてチェッ

クされる。

検証の全てが成功した場合、A Sは、

1. 請求書を生成し、この請求書を完全なものにし、それをファイルに記憶するO C Sに送る。このファイルは、後で、処理(顧客の実際の課金)のためにS M Sに送られる;および
2. 主に新規の購入限界を設定するためにデータベースを更新する。

この「O Kならば請求書をチェックし生成する」機構は、加入者が単一接続中に要求できる各コマンドのために適用する(単一セッションの例えば5つの映画を注文することができる)。

A Sは、S M Sによって保持される情報量と比較して、加入者に関する減少された情報量を有することに注目するべきである。例えば、A Sは、加入者の名前

あるいはアドレスを保持しない。一方では、ASは、加入者のスマートカード番号、加入者の消費者カテゴリー（それで、異なるオファーは異なる加入者に対して行うことができる）、例えば、加入者がクレジットで購入できるか、あるいは加入者が資格を一時的に取り上げられるかあるいは加入者のスマートカードが盗まれたかどうかなどを示す様々なフラグを保持する。減少された情報量の使用は、特定の加入者要求を許可するのにかかる時間量を減少させるのに役立つことができる。

DBAS 3206の主目的は、アクセスを平行させることによってASから見たデータベース性能を増加させることにある（それで、実際、唯一のDBASを有する配置を定義することはあまり意味がない）。ASパラメータは、どれくらいの数のDBASを接続すべきであるかを決定する。所与のDBASは1つのASに接続されてもよい。

OCS 2307は、主にPPVコマンドを処理する。OCS 2307は、いくつかのモードで作動する。

まず第一に、OCS 2307は、製品リフレッシュメント（例えば、請求書がSMSによって既に記憶されているならば、請求書はOCSによって生成されない）、スマートカード3020におけるウォレットの更新、およびセッションキャンセル／更新のような、SMSによって出されたコマンドを処理するように作

動する。

手順における様々なステップは、

1. 関連加入者を（AS 3202を使用して）識別すること；
2. 有効の場合、適当なEMMを送るためにメッセージ発生器に対する適切なコマンドを生成する。コマンドは、

製品コマンド、

ウォレットの更新、

セッション削除

であってもよい。

課金はSMSから既に識別されるので、これらの操作は課金情報の作成を意味

しないことに注目すべきである。これらの操作は「無料製品」購入に適合される。

第二に、OCSは、通信サーバ3022を通して加入者から受信されたコマンドを処理する。これらは、受信機/デコーダ2020に接続されたモデムを介して、あるいは電話4001を介する音声起動によって、あるいは使用可能な場合、ミニテル(MINITELE)、プレステル(PRESTEL)、または同様なシステムを介するキー起動によってのいずれかで受信されてもよい。

第三に、OCSはSMSによって発されたコールバックリクエストを処理する。これらの最後の2つの動作モードは次により詳細に述べられる。

前述の第2の種類のモードでは、OCSは、通信サーバ3022を通してエンドユーザ(加入者)から直接受信されたコマンドを処理することが示される。これらは、製品注文(例えば、特定のPPVイベントのためのものである)、加入者によって要求された加入変更、および親コードのリセット(親コードは、親が所定のプログラムあるいはプログラムのクラスへのアクセス権利を制限できるコードである)を含む。

これらのコマンドが処理される方法は、次に図11を参照してより詳細に述べられる。

加入者による製品注文は下記のステップを含んでいる。

1. CS3022を通して電話をかけ、特定の製品を注文する電話のかけ手をASによって識別する。
2. ASを再び使用して、電話のかけ手の要求妥当性をチェックすること(注文が受信機/デコーダ2020を使用して行われる場合、これはスマートカード3020細部を検証することによって実行される)。
3. 購入の価格を確認する。
4. 価格が電話のかけ手のクレジット制限等を超えないことをチェックする。
5. ASからの部分請求書を受け取る。
6. 完成された請求書を形成するために付加欄を請求書に記入する。
7. 後処理のために完成された請求書を課金情報記憶ファイル3212に追加す

る。

8. 対応するコマンドをPPVメッセージ発生器3210に送り、関連EMMを生成する。

消費者が受信機／デコーダ2020（さらなるこの詳細は後述される）を使用して製品注文をした場合、EMMは、モデムライン4002で送信されるかあるいは放送されるかのいずれかである。これの1つの例外は、モデム接続になんらかの障害がある場合である（消費者が受信機／デコーダを使用して注文をする場合）。すなわち、この場合、EMMは大気を介して放送される。

加入者によって要求された加入変更は下記を含む。

1. 電話のかけ手を（ASを使用して）識別すること
2. 情報をコマンドインタフェースに送る；次に、CIはこの情報をSMSに転送する；および
3. CIを通して、次に、OCSは、（変更が可能であるならば、変更のコストに関して）SMSからの回答を受信する。

変更が受信機／デコーダを使用して要求されるならば、OCSは、SMSの確認を発生する。さもないと、例えば、電話あるいはミニテル(MINTEL)の場合、加入者は、確認のためにプロンプトされ、この回答は、OCSおよびCIを介してSMSに送られる。

親コードのリセットは下記を含む。

1. 電話のかけ手を（ASを使用して）識別すること。および
2. コマンドをMGに送り、適当なりセットパスワードを含む適当なEMMを発生する。

親コードのリセットの場合、コードをリセットするコマンドは、受信機／デコーダから生じることが許可されない安全理由のためである。SMS、電話およびミニテル等だけがこのようなコマンドを生じ得る。したがって、この特定の場合、EMMは、決して電話回線ではなく、大気でのみ放送される。

通信サーバがSAS、および特にOCSに直接接続されているので、ユーザがSAS、および特にOCSおよびASへ直接アクセスすることができることがO

C Sの異なる動作モードの前述の例から理解される。この重要な特徴は、ユーザがユーザのコマンドをS A Sに通信する時間を減らすことに関している。

この特徴は、図12をさらに参照して示されている。この図から、エンドユーザのセット・トップ・ボックス、および特に受信機／デコーダ2020は、S A S 3002に関連した通信サーバ3022と直接通信する機能を有する。S A S 3004を通るエンドユーザからS A S 3002の通信サーバ3022への接続の代わりに、この接続は直接S A S 3002に対するものである。

実際、直接述べられているように、2つの直接接続が備えられる。

第1の直接接続は、エンドユーザが一連の音声コマンドあるいはコード番号をなお入力しなければならないが、S M S 3004を介する通信と比較して時間が節約される電話4001および適切な電話回線を介する音声リンク（および／または使用可能である場合、ミニテルあるいは同様な接続）によるものである。

第2の直接接続は、受信機／デコーダ2020からのものであり、データの入力は、自分自身のドータースマートカード3020を挿入するエンドユーザによって自動的に実行されるので、かかる時間およびこの入力を行う際のエラーの可能性を減らす関連データを入力しなければならないジョブからエンドユーザを解放する。

上記の論議から生じる他の重要な機能は、結果として生じるE M Mが、選択された製品のエンドユーザによって観察し始めるためにエンドユーザに送信されるのにかかる時間を減らすことに関する。

広義の用語において、図12を参照すると、この機能は、再度、S A S 3002に関連した通信サーバ3002と直接通信する機能をエンドユーザの受信機／デコーダ2020を与えることによって実行される。

前述のように、複合受信機／デコーダ2020は、モデムバックチャネル4002によって通信サーバ3022に直接接続されるので、デコーダ2020からのコマンドは、S A S 3022によって処理され、（E M Mを含む）メッセージが生成され、それからバックチャネル4002を通してデコーダ2020に直接送り返される。プロトコルは、C S 3022と受信機／デコーダ2020との間

の通信に使用されるので（後述される）CSは、関連EMMの受信肯定応答を受信し、それによってこの手順に确实性を加える。

したがって、例えば、プレブックモードの場合、SAS3002は、エンドユーザからスマートカード・デコーダ2020を介してそのモデムおよび電話回線4002を介してメッセージを受信し、特定のイベント／製品へのアクセスを要求し、適当なEMMを電話回線4002およびモデムを介してデコーダ2020に戻す。このモデムおよびデコーダは、セット・トップ・ボックス（STB）と一緒に置かれることが好ましい。

したがって、これは、エンドユーザがイベント／製品を見ることができるようマルチプレкса・スクランブラ2004、アップリンク2012、衛星2014およびデータリンク2016を介してMPEG-2データストリーム2002におけるEMMを送信する必要なく達成される。これは時間およびバンド幅に関してかなり節約できる。加入者が自分の買物のために支払うや否や、EMMは受信機／デコーダ2020に到達する実際上の确实性がもたらされる。

前述のOCS3207の第3のタイプの動作モードにおいて、OCSはSASによって出されたコールバックリクエストを処理する。これは図13に関して示される。典型的なコールバックリクエストは、SASが受信機／デコーダに要求する情報とともに、SASを受信機／デコーダ2020がモデムバックチャネル4002を介してコールバックすることを确实にする目的を有する。

コマンドインタフェース3102によって命令されるように、加入チェーンメッセージ発生器3106は、コールバックEMMを生成し、受信機／デコーダ2020に送信する。

このEMMはセキュリティの理由で暗号化装置3008によって暗号化される。

受信機／デコーダが明確に要請されないで、コールバックを単独で起動し、実行すべきである時間／日付をEMMは含んでもよい。すなわち、EMMはまた、一般的には、端末がダイヤルしなければならない電話番号、失敗した呼び出しの後の他の試みの数および2つの呼び出しの間の遅れを含んでもよい。

EMMを受信する場合、あるいは特定の時間・日付で、受信機／デコーダは通信サーバ3022に接続する。OCS3207は、AS3202を使用して電話のかけ手を最初に識別し、スマートカードオペレータおよび加入者詳細のような所定の詳細を検証する。

次に、OCSは、様々な暗号化情報（例えば、関連セッション数、いつセッションが観察されるか、何回加入者が再びセッションを見るために許可されるか、セッションが観察される方法、残りのトークン数、プレブックセッション数等）を送信するようにスマートカード3020に要求する。この情報は、再び暗号化装置3008を使用して、PPVチェーンメッセージ生成器3210によって暗号解読される。

OCSは、後で処理し、SMS3004に送るためにこの情報をコールバック情報記憶ファイル3214に追加する。この情報はセキュリティ理由のために暗号化される。全手順は、スマートカードから読み取られる以上の何物でもなくなるまで繰り返される。

コールバック機構の1つの特定の好ましい機能は、スマートカードを読み取る前（前述のようにAS3202を使用して電話のかけ手の識別直後）、受信機／デコーダが海賊版あるいはコンピュータシミュレーションよりもむしろ本当に本物であるかのチェックがSAS3002によって行われることである。このようなチェックは下記のように実行される。SASは、受信機／デコーダによって受信され、暗号化され、それからSASに戻される乱数を生成する。SASはこの数を暗号解読する。暗号解読が成功し、元の乱数が引き出されるならば、受信機／デコーダが本物であると決定され、手順が続く。さもなければ、手順が中止される。

コールバック中に生じる得る他の機能は、スマートカードのものは使用されていないセッションの削除あるいはウォレットの充電である（これは後で、「スマートカード」というタイトルの節の下で後述される）。

さらに、ペイ・パー・ビューチェーン領域3200に関して、通信サーバ3022の説明が次に行われる。ハードウェアレベルで、これらは、DECの4つの

並列プロセッサマシンを備えている。ソフトウェアアーキテクチャレベルで、図14を参照すると、多数の点で通信サーバは通常のものである。従来の設計からの1つの特別の逸脱は、サーバが受信機／デコーダ2020および従来の電話4001、多分ミニテルあるいは同様なシステムをも有する音声通信の両方に役立つという事実から生じる。

送る際に、2つの注文集中化サーバ3207が（「OCS1」および「OCS2」のように）図14に示されることが注目される。当然、任意の所望の数が与えられてもよい。

通信サーバは、2つの主サーバ（「CSUおよび「CS2」）ならびに多数のフロントルサーバ（「フロントル1」および「フロントル2」）を含む。すなわち、2つのフロントルサーバが図に示されているが、一般的には、主サーバ毎に10あるいは12が備えられてもよい。

確かに、2つの主サーバCS1およびCS2および2つのフロントルサーバ、フロントル1およびフロントル2が示されているけれども、任意の数を使用できる。何らかの冗長性は通常望ましい。

CS1およびCS2は、高レベルTCP/IPリンク3230を介してOCS1およびOCS2に結合されるのに対して、CS1およびCS2は、他のTCP/IPリンクを介してフロントル1およびフロントル2に結合されている。

図示されるように、CS1およびCS2は、「SENDER」（送信）、「RECEIVER」（受信）、「VTX」（ミニテル、プレステル等）、「VOX」（音声通信）、および「TRM」（受信機／デコーダとの通信）のためのサーバを備えている。これらは、フロントルサーバへの信号の通信のために「BUS」に結合されている。

CS1およびCS2は、X25公衆ネットワーク共通プロトコルを使用してそのモデムバックチャネル4002を介して受信機／デコーダ2020と直接通信する。通信サーバ3022と受信機／デコーダ3020との間の比較的低いレベ

ルのプロトコルは、1つの好ましい実施例では、V42標準国際CCITTプロトコルに基づいている。このV42標準国際CCITTプロトコルは、エラー検

出機構およびデータ再伝送機構を有することによって信頼性をもたらし、再伝送の完全性をチェックするためにチェックサムルーチンを使用する。エスケープ機構も、不許可文字の伝送を防止するために備えられる。

一方、音声電話通信は、各々が、高速「T2」(E1)標準電話通信システムのISDN回線を介して接続部3234からローカル電話ネットワークへの約30の同時音声接続を続けることができるフロントル通信サーバを介して実行される。

通信サーバのソフトウェア部の3つの特定の機能(もちろん、その代わりにハードウェアで十分実現できる)は、まず第一に受信機/デコーダから受信された比較的低いレベルのプロトコル情報をOCSへの比較的高いレベルのプロトコル情報に変換することであり、第二に、行われた同時接続の数を減じるかあるいは制御することであり、第三に、混合せずにいくつかの同時チャンネルを備えることにある。この最後の点では、通信サーバは実際、通信チェーン中に使用される、所与のセッションID(識別子)によって規定されている特定のチャンネルにおける対話に関してマルチプレクサの形式の役割を演じる。

最後に、ペイ・パー・ビューチェーン領域3200に関しては、再び、図5を参照すると、プログラム放送のためのサーバ(SPB)3208は、1つあるいはそれ以上のプログラム放送器3250(一般的には、SASから離れて置かれる)に結合され、プログラム情報を受け取る。SPBは、PPVイベント(セッション)に対応する情報を他の使用のためにフィルタリング出力する。

特に重要な機能は、フィルタリングプログラムイベント情報がSPBによってMGに送られることであり、このMGは同様に指令(制御コマンド)をMEに送信し、EMMの周期的放出の速度を所与の状況で変える。すなわち、これは、関連セッション識別子を有する全てのEMMを検出し、このようなEMMに割り当てられたサイクル速度を変え、MEによって行われる。

この機能は特定のEMMに対するバンド幅の動的割り当てとみなすことができる。周期的EMM放出は、EMMインジェクタに関連して下記の節でより詳細に

検討される。

サイクル速度が変えられる状況は、次に図15を参照して述べられる。この図15は、特定のPPVプログラムイベント前からイベントの終了までの短い期間（約10分）、いかにサイクル速度3252が、これらの時間にPPVイベントに対する予想される余分のユーザ要求を満たすために30分毎に約1回の遅いサイクル速度から30秒～1分毎に約1回の速いサイクル速度に上昇されるかを示している。このように、バンド幅は予想されるユーザ要求により動的に割り当てることができる。これは全バンド幅要求を減らすことを助けることができる。

他のEMMのサイクル速度は変更することもできる。例えば、加入EMMのサイクル速度は、適切なビットレート指令を送信するマルチプレクサ・スクランブラ2004によって変更できる。

EMMインジェクタ

EMMインジェクタ3300に関しては、EMMインジェクタの一部を形成し、メッセージ生成器のための出力手段としての役目を果たすメッセージ放出器3302～3308の詳細は、次に図16を参照して述べられる。その機能は、EMMを処理し、これをそれぞれのリンク3314および3316を介してソフトウェアマルチプレクサ3310および3312に、それからハードウェアマルチプレクサ・スクランブラ2004に周期的に（カルーセルの方法で）送ることにある。応答において、ソフトウェアマルチプレクサ・スクランブラ2004は、グローバルビットレート指令を生成し、EMMの全サイクリング速度を制御する。そうするために、MEは、サイクル時間、EMMのサイズ等のような様々なパラメータを考慮する。この図において、EMM_XおよびEMM_Yは、演算子XおよびYに対するグループEMMであるのに対して、EMM_Zは、演算子Xあるいは演算子Yのいずれかに対する他のEMMである。

更なる説明はメッセージ放出器の中の典型的なメッセージ放出器に対して進める。すなわち、残りのMEが同様に作動することが理解される。MEは、MGからの指令の制御の下で、EMMがPPV EMMであるならば、最も著しい送信開始・停止時間および放出速度、ならびにセッション数を操作する。放出速度に関して、好ましい実施例では、関連指令は、非常に速いから非常に遅いまでの5

つの値の中から1つを処理してもよい。数値が指令で特定されるのではなく、むしろMEが、指令をSASの関連部分によって供給される実際の数値にマッピングする。好ましい実施例では、5つの放出速度は下記の通りである。

1. 非常に速い - 毎30秒
2. 速い - 毎分
3. 中間 - 毎15分
4. 遅い - 毎30分
5. 非常に遅い - 毎30分

MEは、第1および第2のデータベース3320および3322を有する。第1のデータベースは、その放送日付をまだ達成していないこれらのEMMのためのものである。すなわち、これらは一連の年代順ファイルをデータベースに記憶されている。第2のデータベースは、中間放送用EMMのためのものである。

システムクラッシュの場合、MEは、関連記憶ファイルを再読み出し、正しい放送を実行する能力を有するように構成されている。データベースに記憶された全てのファイルは、MEが入来指令とMEに既に送信されたEMMとの間の整合性を保持することを望む場合、MGからの要求と同時に更新される。実際放送されているEMMはランダムアクセスメモリ3324にも記憶される。

メッセージ生成器におけるFIFO3162および3164およびメッセージ放出器におけるデータベース3320および3322の組み合わせは、これらの2つの間のリンク3166が一時的に遮断される場合、2つがスタンドアロンで作動できることを意味する。

ソフトウェアマルチプレクサ(SMUX)3310および3312は、MEとハードウェアマルチプレクサ2004との間にインタフェースを与える。好ましい実施例では、一般に1つのSMUXと接続することができるMEの数には制限がないけれども、ソフトウェアマルチプレクサ(SMUX)3310および3312の各々はMEの中の2つからEMMを受信する。SMUXは、EMMを集中し、それからこのEMMをEMMの種類に従って適切なハードウェアマルチプレ

クサに送る。ハードウェアマルチプレクサは異なる種類のEMMを受け入れ、こ

れらをMPEG-2ストリームの異なる位置に配置するためにこれは必要である。SMUXもハードウェアマルチプレクサからのグローバルビットレート指令をMEに転送する。

MEの1つの特定の重要な機能は、MEがランダム順序でEMMを放出することにある。このための理由は下記の通りである。メッセージ放出器は、マルチプレクサに放出することを検出するかあるいは制御する能力を全く有しない。したがって、メッセージ放出器は連続して受信機/デコーダ2020によって受信され、復号化されるべき2つのEMMを送信できる可能性がある。

このような状況では、さらに、EMMが十分分離されない場合、受信機/デコーダおよびスマートカードがEMMの中の二番目を検出し、適切に復号化できない可能性がある。周期的にEMMをランダム順序に放出することでこの問題は解決できる。

ランダム化が実行される方法は、次に図17に関して述べられる。好ましい実施例では、必要なソフトウェアロジックはADAコンピュータ言語で実行される。ランダム化の特別の重要な部分は、データベース3320および3322（バックアップ目的のために使用される）およびRAM3324へのEMMの正しい記憶である。

特定のサイクル速度およびオペレータに関しては、EMMは、列3330（例えば、AからZに進む）および列3332における数（0からNまで進む）によって2次元アレイに記憶される。第3の次元は、サイクル速度3334によって追加されるので、サイクル速度と同じ数の2次元アレイがある。好ましい実施例では、256列があり、一般的には各列には200あるいは300のEMMがある。すなわち、5サイクル速度がある。アレイの最終次元は異なるオペレータの存在によって追加される。つまりオペレータと同じ数の3次元アレイがある。この方法でのデータの記憶は、MGが特定のEMMを削除したい場合、迅速な検索を可能にできる。

EMMの記憶は、「ハッシュ」アルゴリズム（特に、「一方向ハッシュ関数」として既知である）により行われる。これはモジュロ方式で操作するので、連続

列は、列におけるより高い数が使用される前に満たされ、各列における EMM の数は、概ね一定のままである。この例は 2 5 6 の列があるものとみなされる。M G が識別子 (I D) 1 を有する EMM を M E に送信する場合、列「1」は、この EMM に割り当てられ、列 3 3 3 0 において最初の数 3 3 3 2 を受け入れる。

I D 2 を有する EMM は列「2」に割り当てられ、列 2 5 6 まで同様に割り当てられる。I D 2 5 7 を有する EMM は、(モジュロ機能に基づいて) 列「1」に再度割り当てられ、第 1 の列における第 2 の数を受け入れ、以下同様にする。

例えば、特定の EMM の削除が M G によって要求される場合、特定の EMM の検索は上記の逆のことによって行われる。ハッシュアルゴリズムは、列を得るために列における数がその後に検出される EMM I D に適用される。

実際のランダム化は、EMM がメッセージ放出国のハードウェアおよび/またはソフトウェアで実行されるランダム化手段 3 3 4 0 を使用して周期的に R A M 3 3 2 4 から検索される。検索はランダムであり、再びハッシュアルゴリズムに基づいている。

まず第一に、乱数 (上記の例においては最初は 1 ~ 2 5 6 の範囲にある) は列における特定の数を生じるように選択される。第二に、他の乱数は列において特定の数を生じるように選択される。他の乱数は、所与の列における EMM の全数により EMM の全数により選択される。所与の EMM が選択され、放送されると、ハッシュ関数を再び使用して R A M 3 3 2 4 における第 2 の同一の記憶領域に移動される。

したがって、第 1 の領域は、EMM が放送されると、サイズが、一旦全列が使用されると、これが削除される程度まで減少する。一旦第 1 の記憶領域が完全に空になると、第 1 の記憶領域は、新しい EMM 放送の循環前に第 2 の記憶領域と取り替えられ、またその逆も行われる。

上記のように、EMM の 2 サイクルあるいは 3 サイクルの後、統計的には、連続して送信される同じエンドユーザに対して望まれる任意の 2 つの EMM の可能性は無視できる。

EMM が記憶されている一定の間隔で、コンピュータ 3 0 5 0 は、記憶装置に

おけるバイト数を計算し、これから、マルチプレクサおよびソフトウェアマルチプレクサからのグローバルビットレート指令を与えた放出のビットレートを計算する。

バックアップデータベース3320および3322に対する参照は上記で行われた。実際、好ましい実施例では、RAM3324の中にあるもののバックアップバージョンを保持するシーケンシャルファイルメモリがある。メッセージ放出器の故障およびその後の再始動の場合、あるいはより一般的にはMEが如何なる理由でも再始動される場合、それを介して記憶されたEMMがRAMにアップロードされるリンクがRAMとデータベースとの間に形成される。このように、故障の場合、EMMを失う危険を取り除くことができる。

列が一般的には所与のオペレータに対応し、列における数がセッション数に対応する場合、PPV EMMの同様な記憶は、加入EMMに関しては前述の記憶装置に生じる。

スマートカード

ドーター、すなわち「加入者」のスマートカード3020は、図18に概略的に示され、使用中受信機／デコーダ2020のカードリーダーの対応する接点のアレイに接続される接点の標準アレイ120に結合される入出力バスを有するモトローラ6805マイクロプロセッサのような8ビットマイクロプロセッサ110を備え、カードリーダーは従来の設計のものである。マイクロプロセッサ110には、好ましくはマスクROM130、RAM140およびEEPROM150に対するバス接続部も装備されている。

スマートカードは、スマートカードの所定の物理的パラメータ、チップ上の接点の位置および外部システム（および特に受信機／デコーダ2020）とスマートカードとの間での所定の通信をそれぞれ決定するので、ここではさらに説明されないISO7816-1、7816-2および7816-3の標準プロトコルに従う。マイクロプロセッサ110の1つの機能は、次に述べられるようにスマートカードのメモリを管理することにある。

EEPROM150は、所定の動的に作成されるオペレータゾーン154、155、156および次に図19を参照して述べられる動的に作成されたデータゾ

ーンを含んでいる。

図19を参照すると、EEPROM150は、スマートカード3020の製造者によって設定される固定加入者スマートカード識別子を含む8バイトの固定「カードID」（すなわち製造者）ゾーン151を備えている。

スマートカードがリセットされる場合、マイクロプロセッサ110は、受信機／デコーダ2020に信号を出す。この信号は、スマートカードによって使用される条件付アクセスシステムの識別子およびカードIDを含むスマートカードに記憶されたデータから発生されたデータを含む。この信号は、スマートカードが受信機／デコーダ2020によって使用された条件付アクセスシステムと適合性があるかを検査するために記憶信号をその後に使用する受信機／デコーダ2020によって記憶される。

EEPROM150は、擬似乱数を発生するプログラムを含む固定「乱数発生器」ゾーン152も含んでいる。このような乱数は、スマートカード3020によって発生されたトランザクション出力信号をさまざまに変化させるために使用され、放送器に送り返される。

乱数発生器ゾーン152の下に144バイトの固定「管理」ゾーン153が装備される。固定管理ゾーン153は、後述されるようにゾーン154、155、156…の動的作成（および除去）においてROM130のプログラムによって利用される特定のオペレータゾーンである。

固定管理ゾーン153は、ゾーンを作成あるいは取り除くスマートカードの権利に関するデータを含んでいる。

ゾーンを動的に作成し、取り除くためのプログラムは、SAS3002によって送信され、受信機／デコーダ2020によって受信され、加入者スマートカード3020に送られる特定のゾーン作成（あるいは除去）EMMに応答する。EMMを作成するために、オペレータは管理ゾーンに専用の特定キーを必要とする。これは一人のオペレータが他のオペレータに関するゾーンを削除することを防止する。

管理ゾーン153の下には、オペレータ1、2…Nのそれぞれに対する一連の「オペレータID」ゾーン154、155、156がある。通常、少なくとも

1つのオペレータIDゾーンは、エンドユーザがこのオペレータによって放送されるプログラムを暗号解読することができるように加入者スマートカード3020のEEPROMにプリロードされる。しかしながら、他のオペレータIDゾーンは、その後に述べられるように、エンドユーザ（加入者）によって自分のスマートカード3020を介して発生されたトランザクション出力信号に応じて管理ゾーン153を使用してその後に動的に作成できる。

各オペレータゾーン154、155、156は、スマートカード3020が属するグループの識別子およびグループ内部のスマートカードの位置を含んでいる。このデータは、スマートカードが（そのグループにおける他のスマートカードとともに）このグループのアクセスを有する（がグループにおけるスマートカードの位置でない）放送「グループ」加入EMMならびにグループ内部のこのスマートカードにのみアドレス指定される「個人」（あるいは商業オファァ加入）EMMに応答することを可能にする。各々のこのようなグループの256のメンバースマートカードがある可能性があるので、この機能はEMMを放送するのに必要なバンド幅を著しく減少させる。

「グループ」加入EMMを放送するのに必要なバンド幅をさらに減らすために、スマートカード3020および他のドータースマートカードのEEPROMにおける各オペレータゾーン154、155、156、および全ての同様なゾーンにおけるグループデータは、例えば、グループのメンバーの削除によって作成された任意の穴を満たすように各グループにおけるその位置を特定のスマートカードができるように連続して更新される。この穴は、STMサーバ3104においてこのような穴のリストがある場合、SAS3002によって満たされる。

このように、断片化が減少され、各グループのメンバーシップは、256人のメンバーの最大にあるいはその近くに保持される。

各オペレータゾーン154、155、156は、EEPROM150に記憶された1つあるいはそれ以上の「オペレータデータオブジェクト」に関連している。図19に示されるように、一連の動的に作成された「オペレータデータ」オブジェクト157～165はオペレータIDゾーンの下に置かれる。これらのオブジェクトの各々は下記のa)、b)、c)でラベル付けされる。

- a) 図19の左側部に示されるように関連オペレータ1, 2, 3...Nに対応する「識別子」1, 2, 3...N
- b) オブジェクトのタイプを示す「ID」
- c) 図19の各関連オペレータオブジェクトの右側部に示されるようにデータのために用意された「データ」ゾーン。オペレータ1のデータオブジェクトにおけるデータのタイプの下記の説明が全て他のオペレータのデータオブジェクトにも適用可能であるように各オペレータは同様なデータオブジェクトのセットに関連することを理解すべきである。さらに、データオブジェクトは、EEPROMの隣接する物理的領域に置かれ、その順序は重要でない。

データオブジェクトの削除は、スマートカードに穴166を形成する、すなわち、削除されたオブジェクトが予め占有されるバイト数は直ちに占有されない。

このように「自由された」バイト数、すなわち「穴」は下記でラベル付される。

- a) 「識別子」0、および
 - b) バイトがオブジェクトを自由に受け取ることができることを示す「ID」
- 作成された次のデータオブジェクトは、識別子0によって識別されるような穴を満たす。このように、EEPROM150の限られたメモリ容量（4キロバイト）は有効に利用される。

次に、各オペレータに関連するデータのセットに向けると、データオブジェクトの例が次に述べられる。

データオブジェクト157は、受信機/デコーダ2020によって受信された暗号化EMMを暗号解読するために使用されるEMMキーを含んでいる。このEMMキーはデータオブジェクト157に永久記憶されている。このデータオブジェクト157は、スマートカード3020の配布前に作成されてもよいし、および/または（前述のように）新しいオペレータゾーンを作成する場合、動的に作成されてもよい。

データオブジェクト159は、エンドユーザが加入した特定のプログラムの「ブーケ」を暗号解読することができるように関連オペレータ（この場合、オペレータ1）によって送信される。新しいECMキーは、（この場合）オペレータ

1からの放送を見るエンドユーザの全権利を更新するグループ加入（更新）EMMとともに、一般的には毎月送信される。

別々のEMMキーおよびECMキーの使用は、見る権利が異なる方法で（この実施例では、加入によりおよび個別的に（ペイ・パー・ビュー））購入することを可能にし、セキュリティも増加する。このペイ・パー・ビュー（PPV）モードはその後述されている。

新しいECMキーは周期的に送られるので、例えば、受信機／デコーダをスイッチオフするかあるいはクロックをリセットし、受信機／デコーダ2020のタイマが無効できるように古いECMキーの満了を防止することによってユーザが古いECMキーを使用することを防止することが重要である。したがって、オペレータゾーン154は、ECMキーの陳腐化日付を含む領域（一般的には2バイトのサイズを有する）を含んでいる。スマートカード3020は、この日付と受信ECMに含まれる現日付とを比較し、現日付が陳腐化日付よりも後である場合、暗号解読を防止するように構成されている。陳腐化日付は、前述のようにEMMを介して送信される。

データオブジェクト161は、加入者が加入した放送オペレータのプログラムの正確な表示である64ビット加入ビットマップを含む。あらゆるビットは、プログラムを示し、プログラムが加入されている場合、「1」をセットし、プログラムが加入されていない場合、「0」をセットする。

データオブジェクト163は、例えば、無料プリビューあるいは他の宣伝に応じて当面の放送を見る権利を買うためにPPVモードで消費者によって使用することができる多数のトークンを含んでいる。データオブジェクト163は、消費者に対するクレジットを可能にするために例えば負の値をセットされてもよい限界値も含む。トークンは、例えば、クレジットによって、およびモデムバックチャネル4002を介して、あるいは例えばクレジットカードと組み合わせて音声サーバを使用することによって購入することができる。特定のイベントは1つのトークンあるいは多数のトークンとして代金を請求できる。

データオブジェクト165は、図20のテーブル167に関して示されるように、PPVイベントの記述を含んでいる。

PPVイベント記述167は、視聴セッションを識別する「セッションID」168（プログラムおよび放送の時間や日付に対応する）と、いかに視聴権が購入されるかを示す「セッションモード」169（例えば、プレブックモードにおいて）と、「セッションインデックス」170と、「セッションビュー」171とを含んでいる。

プログラムをPPVモードで受信することに関して、受信機デコーダ2020は、プログラムがPPVモードで販売されたプログラムであるかどうかを決定する。そうであるならば、デコーダ2020は、プログラムのためのセッションIDがそれに記憶されているかどうかをPPVイベント記述167に記憶された項目を使用してチェックする。セッションIDがそこに記憶されているならば、制御語がECMから抽出される。

セッションIDがそこに記憶されていない場合、特定のアプリケーションによって、受信機/デコーダ2020は、エンドユーザがECMから読み取られるように約25トークンのコストでセッションを見るかあるいはイベントを購入するために通信サーバ3022に接続する権利を有することを示すメッセージをエンドユーザに表示する。

トークンを使用して、エンドユーザが（遠隔コントローラ2026によって（図2を参照））「イエス」と答えるならば、デコーダ2020は、ECMをスマートカードに送信し、スマートカードは、25トークンだけスマートカード3020のウォレットを減らし、PPVイベント記述167におけるセッションID168、セッションモード169、セッションインデックス170およびセッションビュー171を書き込み、ECMから制御語を抽出し、この制御語を暗号解読する。

「プレブック」モードでは、EMMはスマートカード3020に送られるので、スマートカードは、EMMを使用してPPVイベント記述167におけるセッションID168、セッションモード169、セッションインデックス170およびセッションビュー171を書き込む。

セッションインデックス170は、一方の放送と他方の放送とを区別するようにセットできる。この機能は、許可が放送のサブセットに対して、例えば、5つ

の放送の中の3回を与えることを可能にする。PPVイベント記述167に記憶された現セッションインデックス170とは異なるセッションインデックスを有するECMがスマートカードに送られるや否や、セッションビュー171の数は1だけ減らされる。セッションビューがゼロに達する場合、スマートカードは、現セッションインデックスに対して異なるセッションインデックスを有するECMを暗号解読することを拒否する。

セッションビューの初期値は、放送供給者が、関連するイベントを規定することを望む方法によってだけ決まる。すなわち、それぞれのイベントに対するセッションビューは任意の値をとってもよい。

スマートカードのマイクロプロセッサ110は、何時特定のプログラムの視聴数に対する制限に達したかを検出するために計数および比較プログラムを実行する。

PPVイベント記述167におけるセッションID168、セッションモード169、セッションインデックス170およびセッションビュー171は、前述のように「コールバック」手順を使用してスマートカードから抽出されてもよい。

各受信機/デコーダ2020は、この受信機/デコーダを独自に識別するかあるいはその製造者を識別するかのいずれかを行うことができるか、あるいは受信機/デコーダが特定の個人スマートカード、同じ製造者あるいは対応する製造者によって作られた特定の種類のスマートカード、この種の受信機/デコーダと排他的に併用することを目的としている任意の他の種類のスマートカードとだけ作動できるように他の方法で受信機/デコーダを分類できる識別子を含む。このように、1放送供給者によって消費者に供給された受信機/デコーダ2020は、非許可ドータースマートカード3020の使用から守られる。

さらに、またスマートカードと受信機の間にあるこの最初の「ハンドシェーク」の代わりに、スマートカード3020のEEPROMは、スマートカードが機能を果たすことができる受信機/デコーダ2020のカテゴリーを記述するフィールドあるいはビットマップを含むことができた。これらは、スマートカード3020の製造中あるいは特定のEMMによってのいずれかで特定できた。

スマートカード3020に記憶されたビットマップは、各々にスマートカードが使用されてもよいように対応する受信機／デコーダIDで識別される80までの受信機／デコーダのリストを一般的に含んでいる。各受信機／デコーダに関連するのは、スマートカードが受信機／デコーダと併用できるか否かを示すレベル「1」あるいは「0」である。受信機／デコーダのメモリ2024のプログラムは、スマートカードに記憶されたビットマップにおける受信機／デコーダの識別子を検索する。識別子が検出されるならば、識別子に関連した値は「1」であり、それからスマートカードは使用可能にされる。検出されないならば、スマートカードは受信機／デコーダとともに機能を果たさない。

さらに、一般的には、オペレータ間の合意のために、特定の受信機／デコーダにおける他のスマートカードの使用を許可することが望まれる場合、特定のEMMはトランスポンダ2014を介してそのビットマップを変えるためにこれらのスマートカードに送られる。

各放送供給者は、ある種の所定の判定基準により自分の加入者を区別できる。例えば、多数の加入者は「VIP」として分類できる。したがって、各放送供給者は自分の加入者を複数のサブセットに分類でき、各サブセットは任意の加入者数を含む。

特定の加入者が属するサブセットはSMS3004にセットされる。次に、SAS3002は、加入者がスマートカードのEEPROMの約154の関連オペレータデータゾーンの中に属するサブセットに関する情報（一般的には1バイトの長さ）を書き込む加入者に送信する。次に、イベントが放送供給者によって放送されると、一般的には256ビットのECMは、イベントとともに送信され、加入者のサブセットのどれがイベントを見ることができるかを示している。オペレータゾーンに記憶された情報により、加入者がECMによって決定されるようにイベントを見る権利を有していない場合、プログラム視聴が否定される。

この機能は、例えば、特定のプログラム、特に、特定の地理的な地域で行われるスポーツ競技種目に関するプログラムの送信中特定の地理的な地域での所与のオペレータのスマートカードの全てをスイッチオフするために使用されてもよい

。このように、フットボールクラブおよび他のスポーツ団体は、その場所以外の放送権を販売できると同時に地方のスポーツのサポーターがテレビでこの競技種目

を見ることを防止する。このように、地方のサポーターは、チケットを買い、スポーツ競技種目に参加するように勧められる。

ゾーン151～172に関連した機能の各々は、ゾーンの動的作成とは無関係の別個の発明とみなされる。

本発明は、単に例として述べられ、詳細の変更は本発明の範囲内で行うことができる。

説明に開示された各特徴、および（妥当である場合）請求の範囲および図面は、別々にあるいは任意の適切な組み合わせで提供されてもよい。

前述の好ましい実施例では、本発明のある種の特徴はコンピュータソフトウェアを使用して実現された。しかしながら、もちろん、これらの特徴のいずれかはハードウェアを使用して実現されてもよいことは当業者に明らかである。さらに、ハードウェア、コンピュータソフトウェア等によって実行された機能は、電気信号等であるいは電気信号を使用して実行されることは容易に理解される。

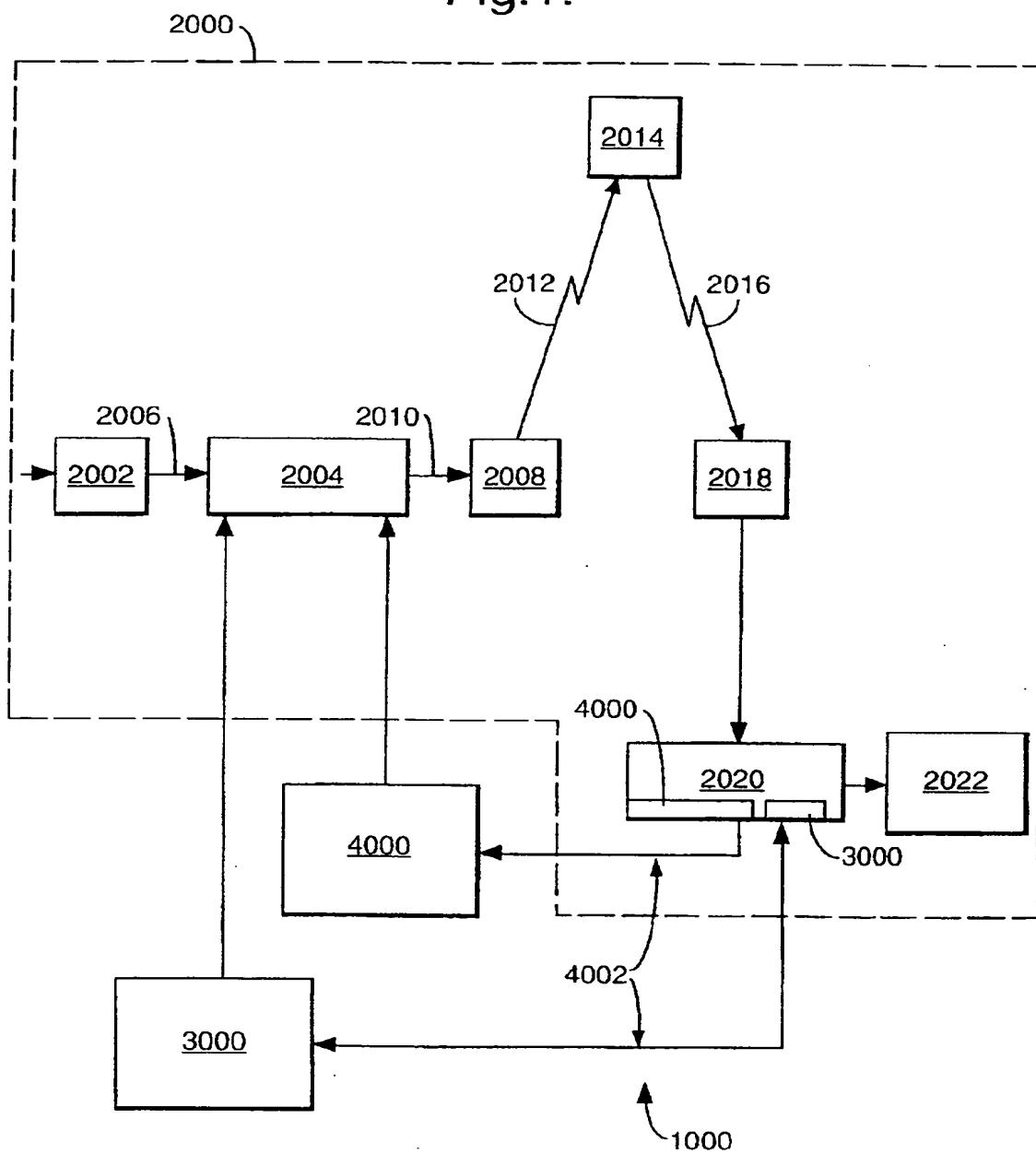
相互参照は、我々の同時係属出願に対して行われ、全ては、同じ出願日を有し、名称が「信号発生および放送（代理人参照番号PC/ASB/19707）」、「暗号化放送信号の受信機と併用するためのスマートカード、および受信機（代理人参照番号PC/ASB/19708）」、「放送・受信システムおよびそのための条件付アクセスシステム（代理人参照番号PC/ASB/19710）」、「受信機／デコーダを介して送信機からコンピュータにコンピュータファイルのダウンロード（代理人参照番号PC/ASB/19711）」、「テレビジョンプログラムおよび他のデータの送信および受信（代理人参照番号PC/ASB/19712）」、「データのダウンロード（代理人参照番号PC/ASB/19713）」、「コンピュータメモリ構成（代理人参照番号PC/ASB/19714）」、「テレビジョンあるいはラジオ制御システム生成（代理人参照番号PC/ASB/19715）」、「送信データストリームからのデータセクシ

ョンの抽出（代理人参照番号PC/ASB/19716）」、「アクセス制御システム（代理人参照番号PC/ASB/19717）」、「データ処理システム（代理人参照番号PC/ASB/19718）」、および「放送・受信システム、およびそのための受信機／デコーダおよび遠隔コントローラ（代理人参照番号PC

／ASB/19720）」である。これらの文書の開示は参照してここに組み込まれている。出願のリストは本出願を含んでいる。

【図1】

Fig.1.



【図2】

Fig.2.

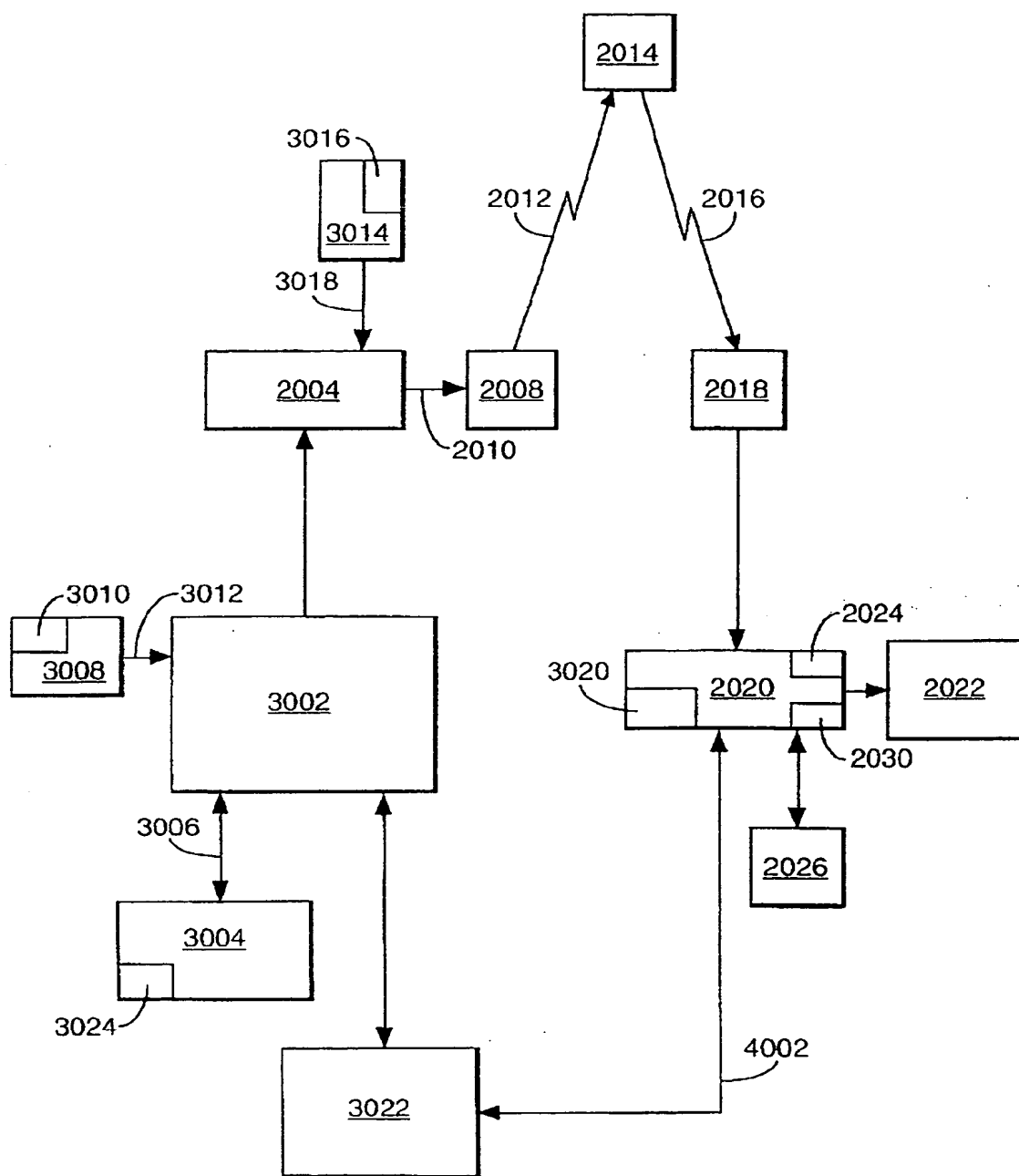
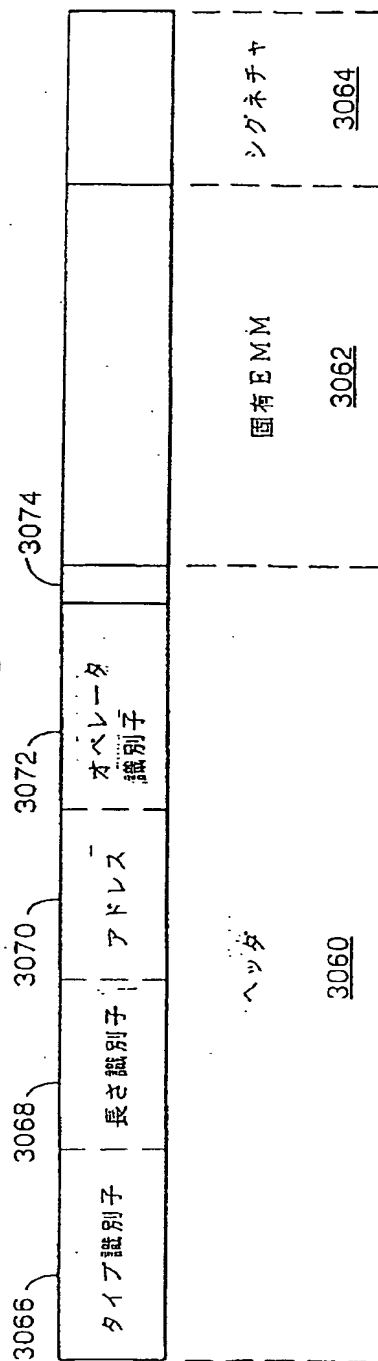
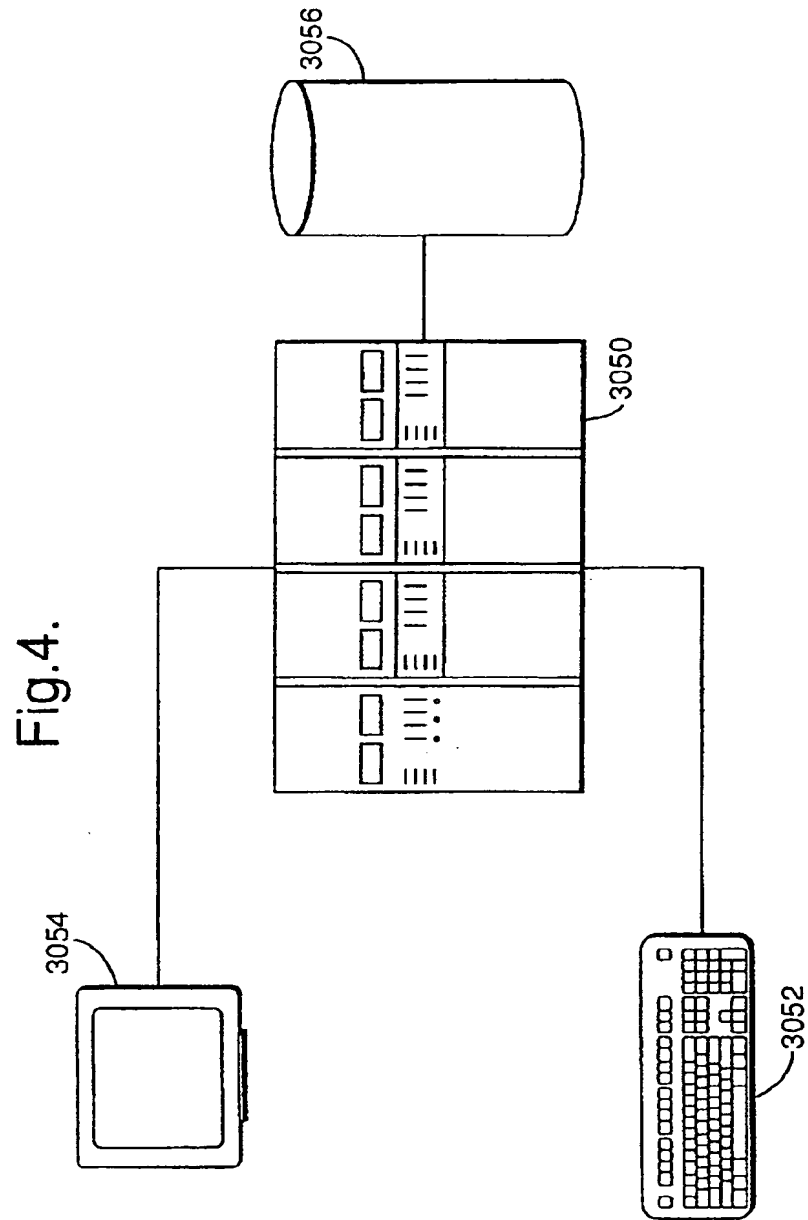


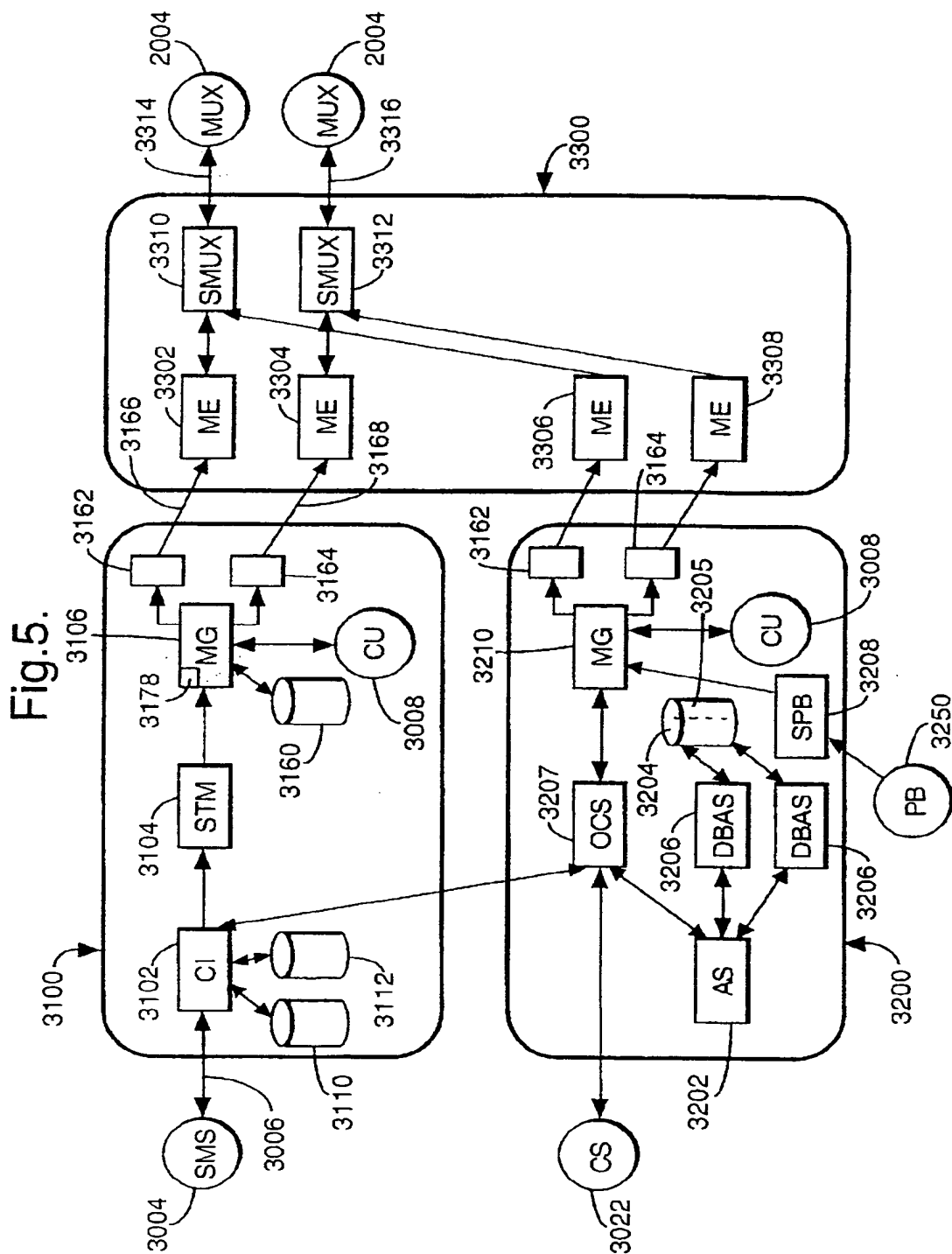
Fig.3.



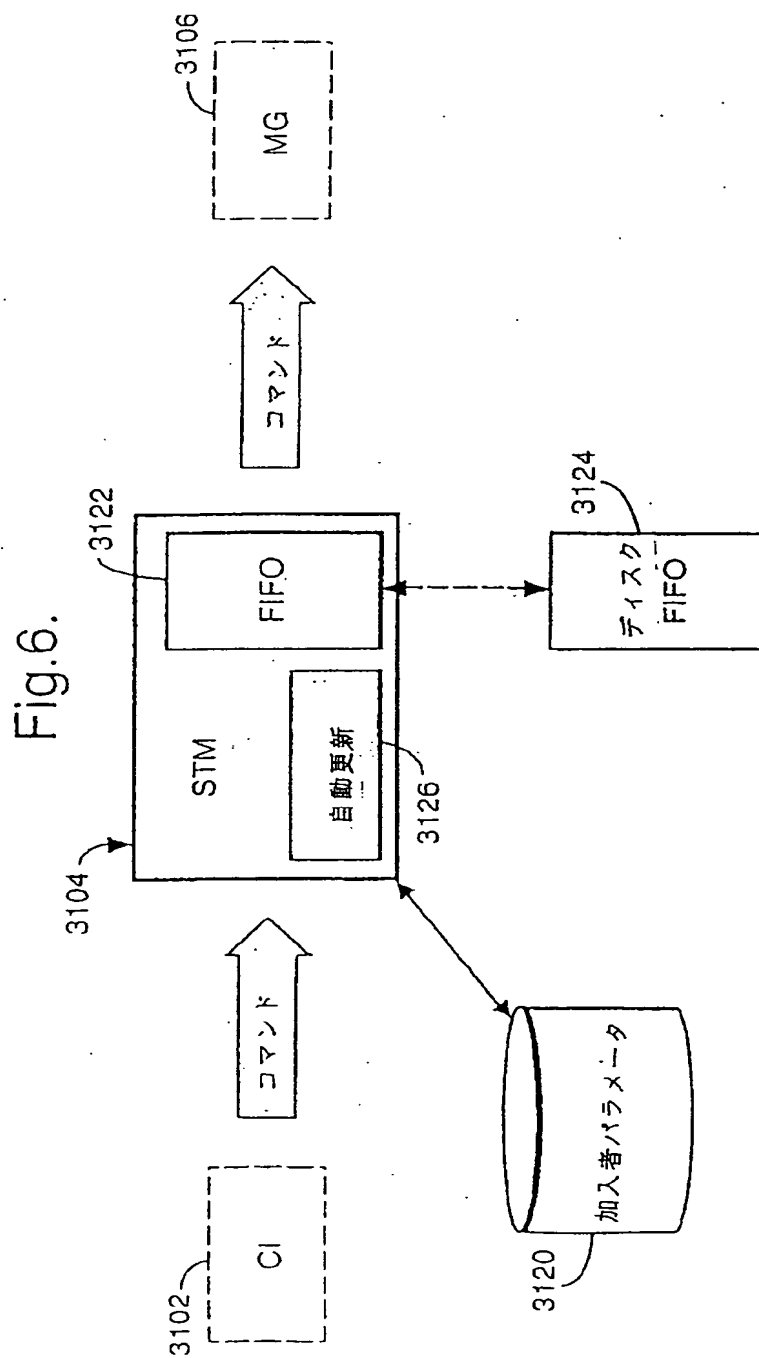
【図4】



【図5】

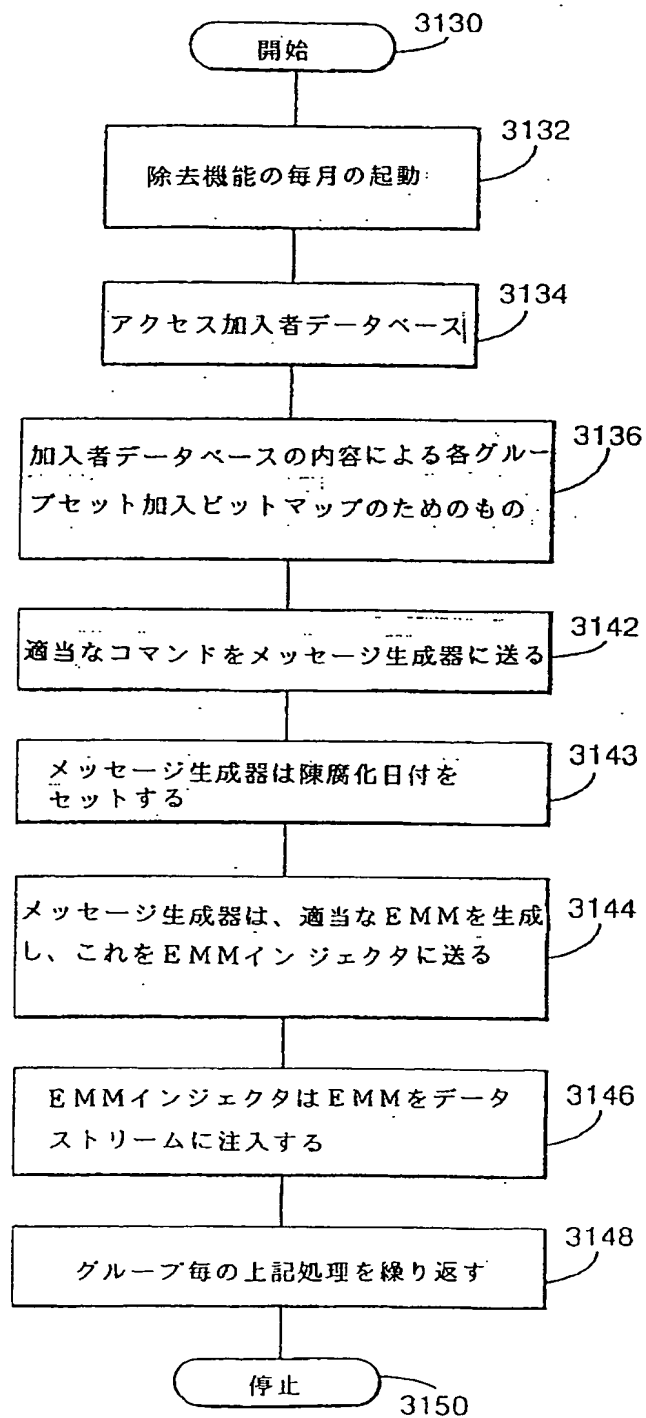


【図6】

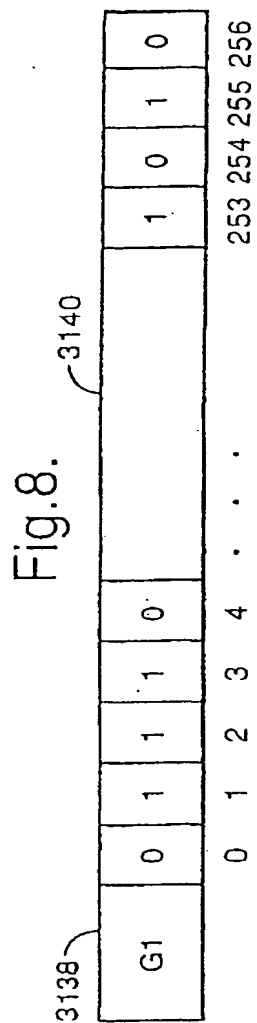


【図7】

Fig.7.



【図8】



【図 9】

Fig.9.

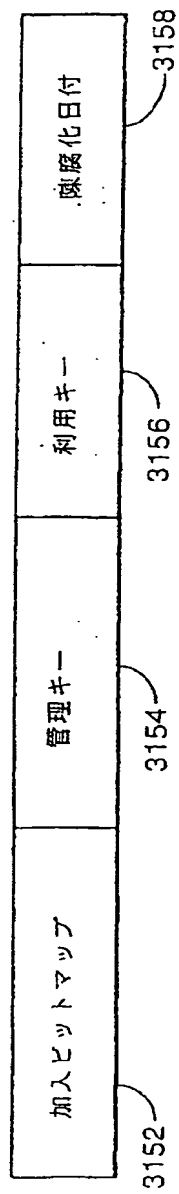
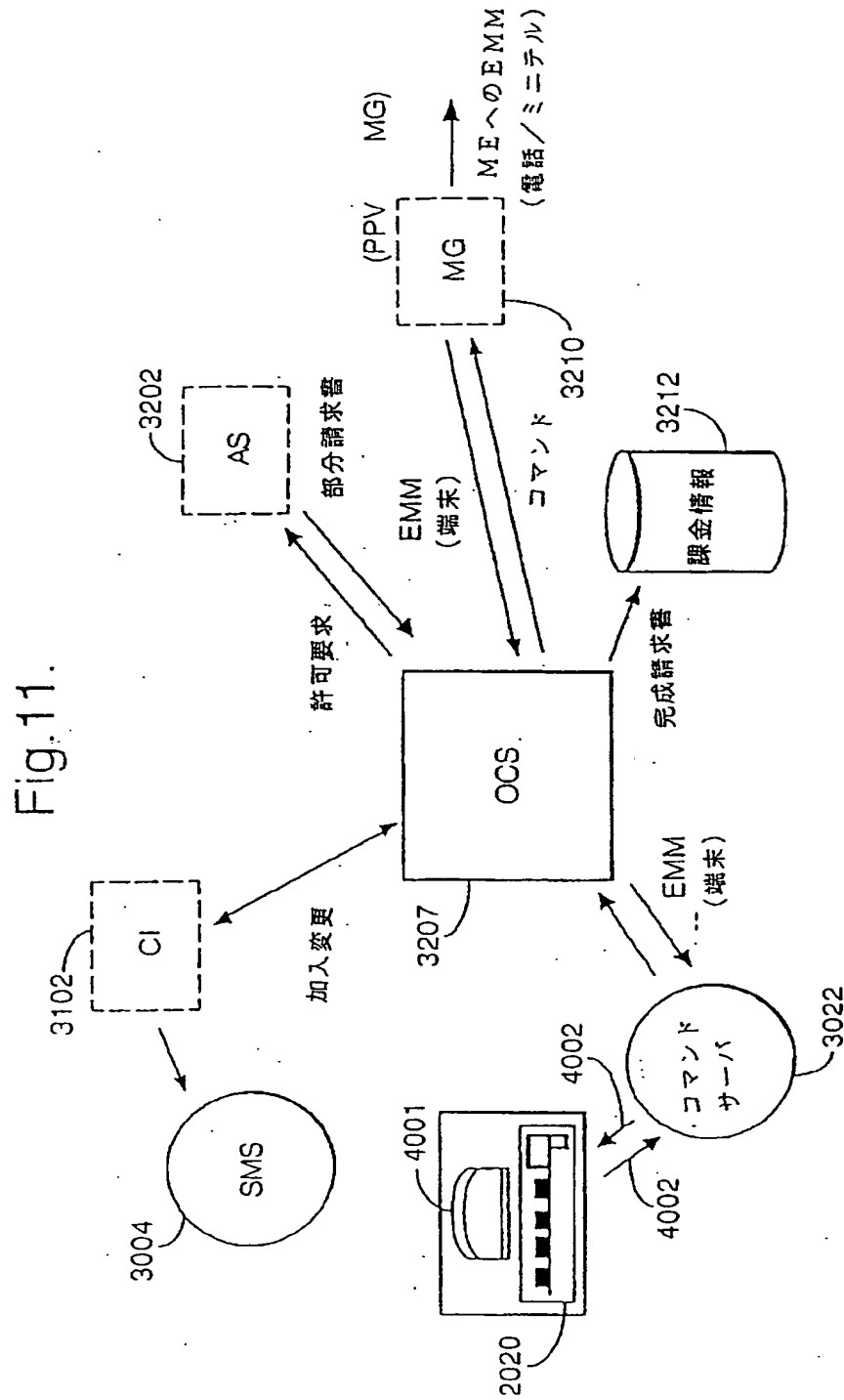


Fig.10.

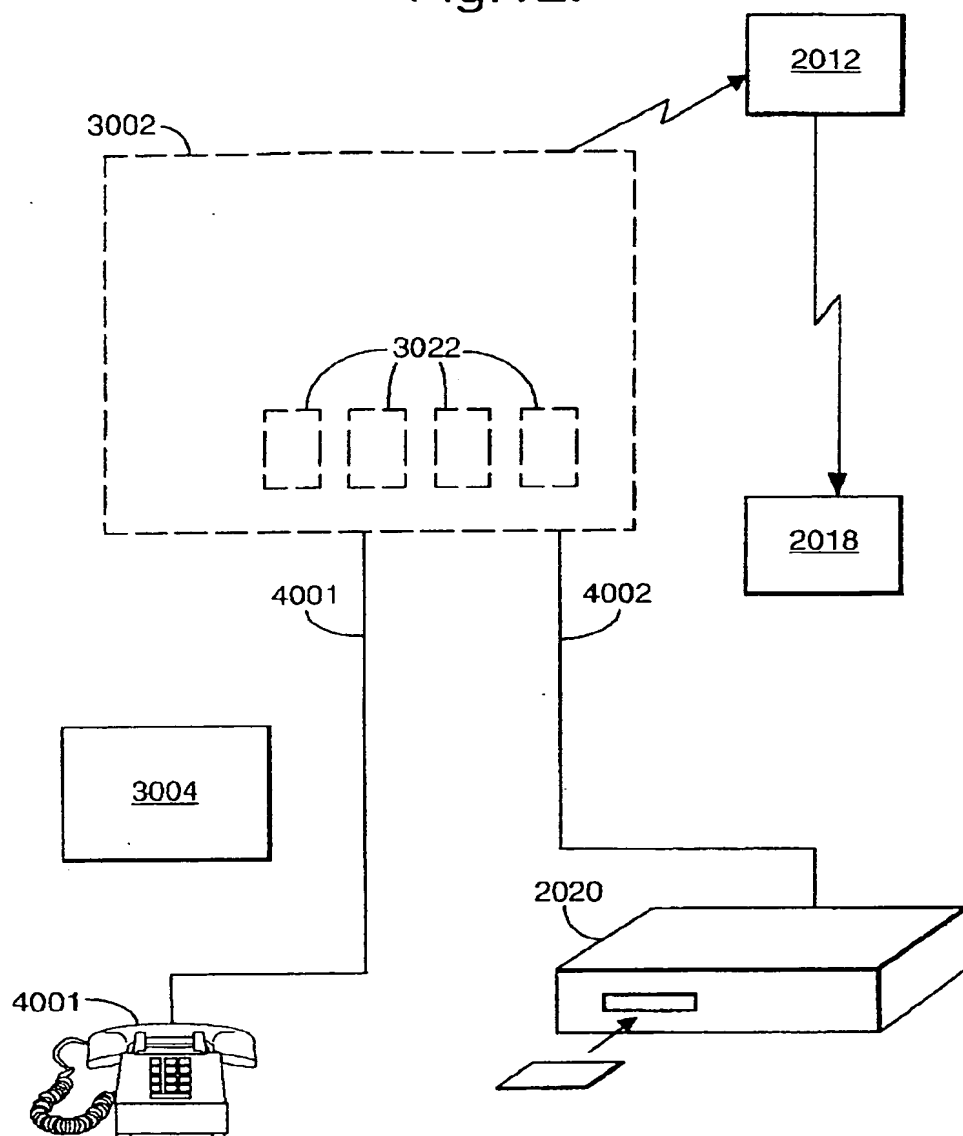
PID 3170			
	ID 3172	長さ 3174	セッション番号
ヘッダ 3060	固有 EMM 3062		シグネチャ 3064

【図11】

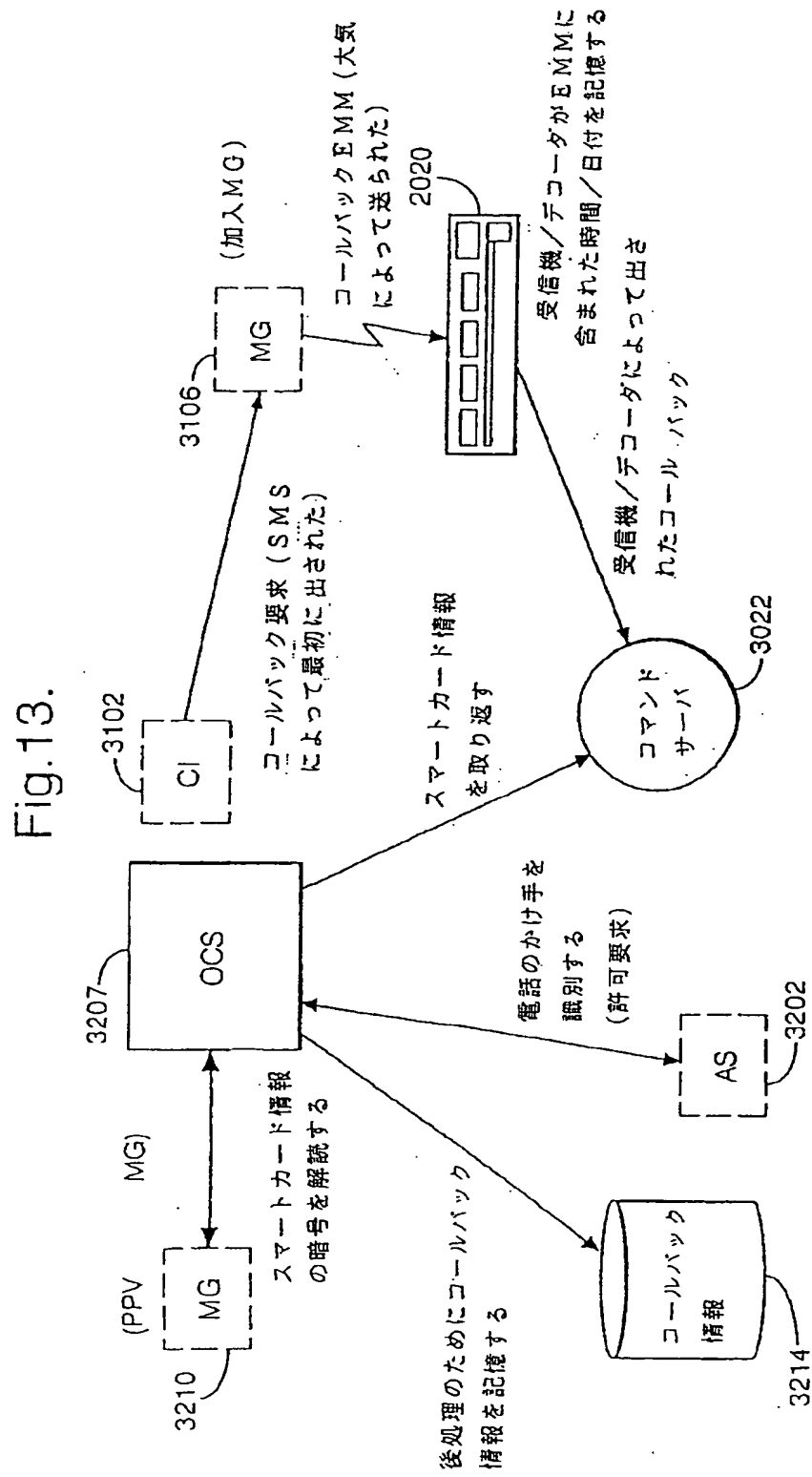


【図12】

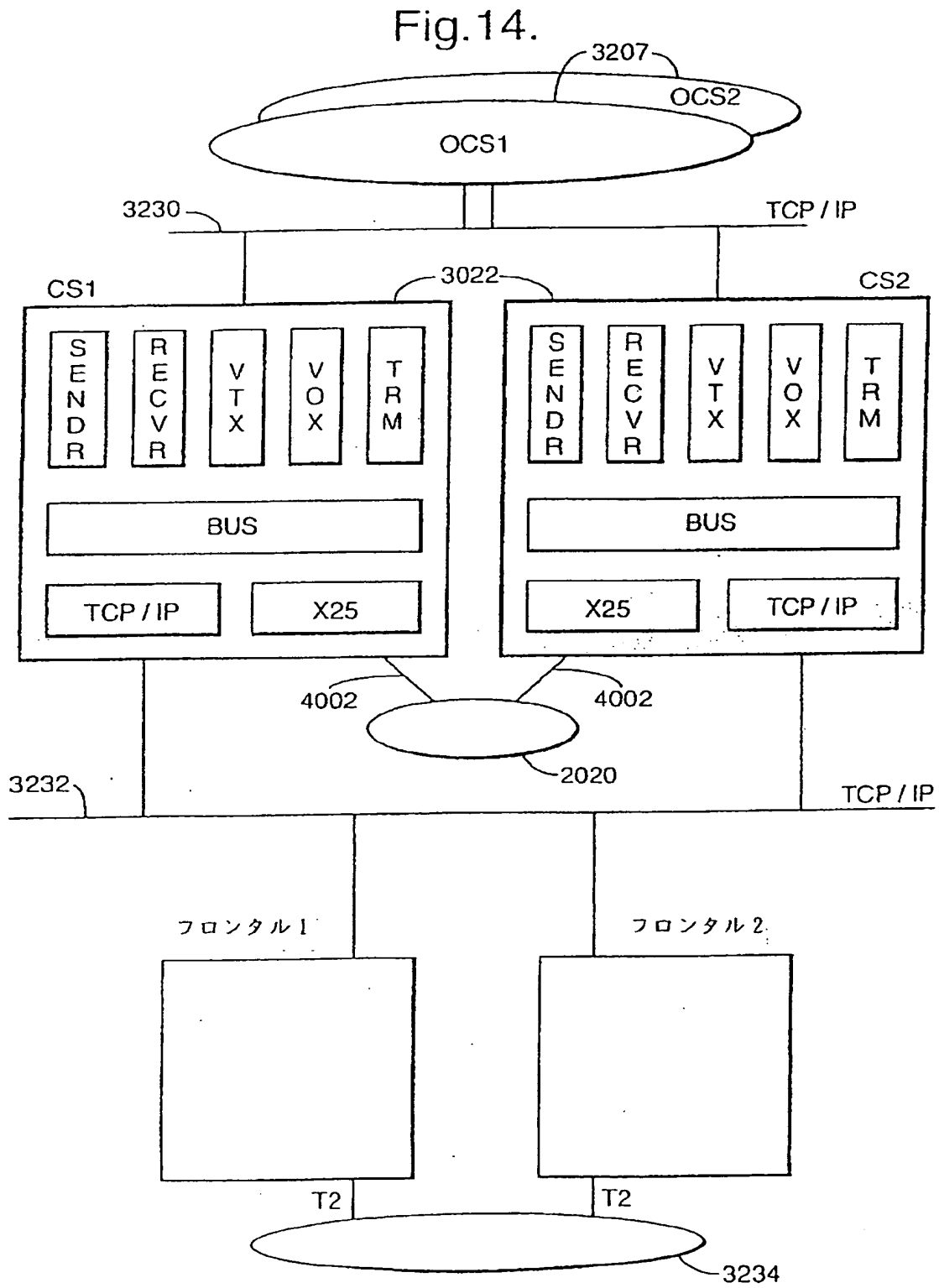
Fig.12.



【図13】

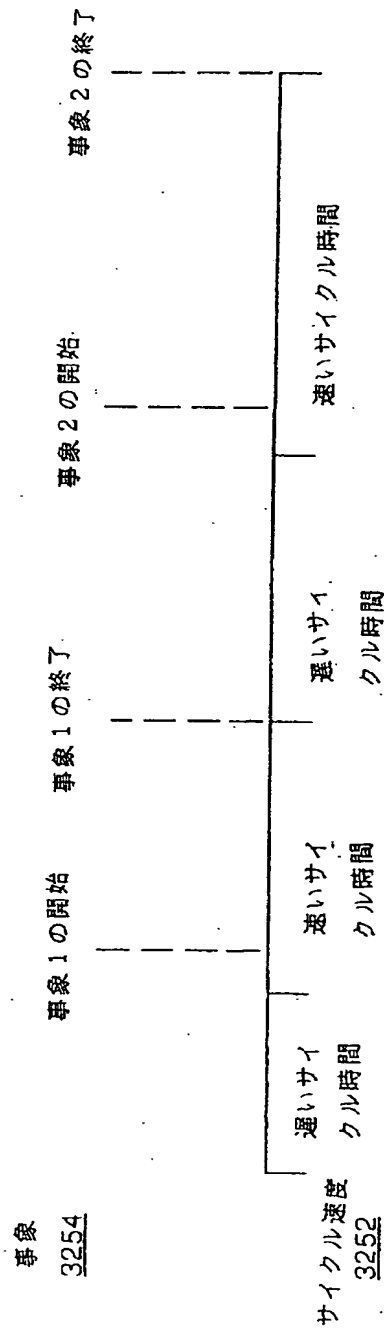


【図14】



【図15】

Fig.15.



【図16】

Fig.16.

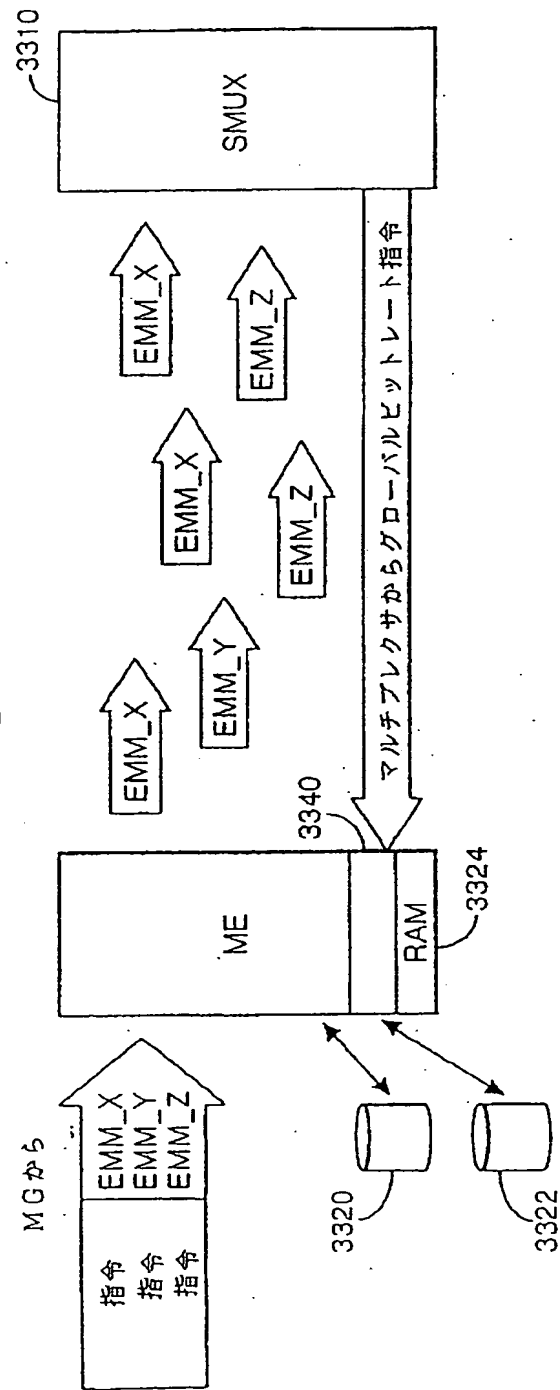
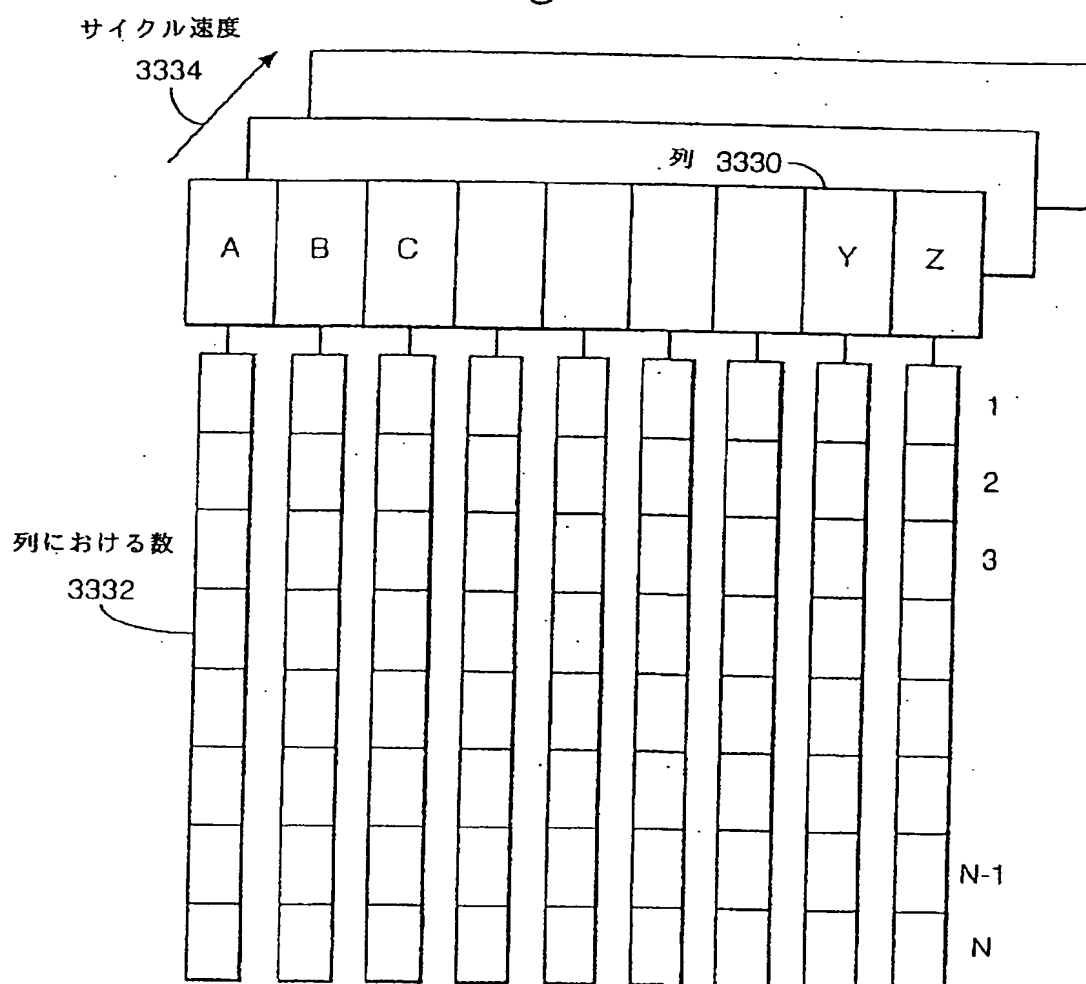
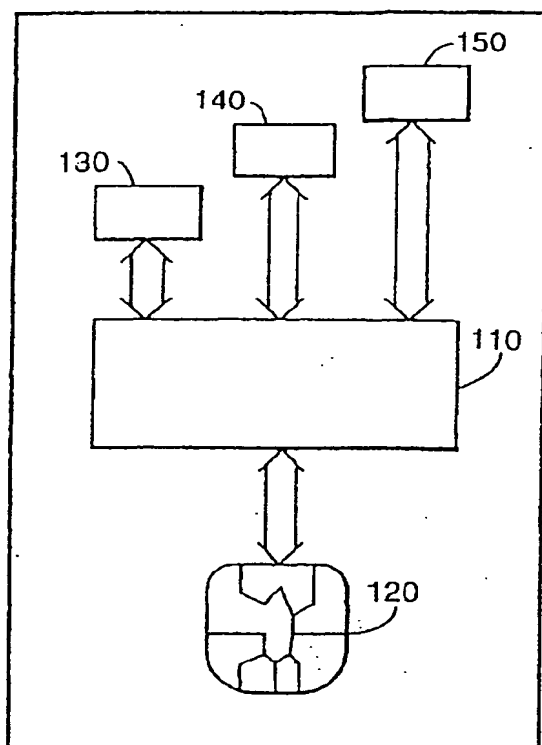


Fig.17.



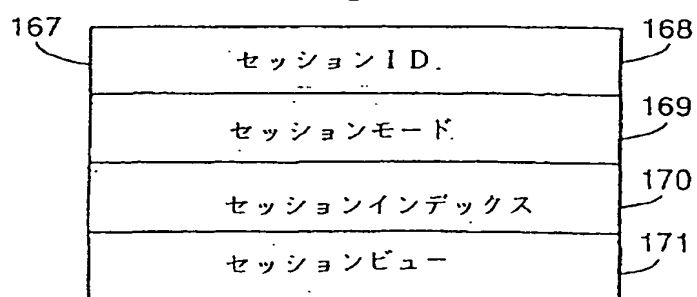
【図18】

Fig.18.



【図20】

Fig.20.



【図19】

Fig.19.

カードIDゾーン			151
乱数発生器ゾーン			152
管理ゾーン			153
オペレータ 1 ID			154
オペレータ 2 ID			155
⋮			
オペレータ N ID			156
1	EMM キー	データ	157
1	ECM キー	データ	159
2	EMM キー	データ	
1	加入ビット マップ	データ	161
0	オブジェク ト無し		166
3	ECM キー	データ	
1	トークン ウォレット	データ	163
1	PPV事象	データ	165
⋮			
N	ECM キー	データ	

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No. PCT/EP 97/02107		
A. CLASSIFICATION OF SUBJECT MATTER IPC 6 H04N7/16 H04N7/167		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 6 H04N		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages Relevant to claim No.	
X	US 5 144 663 A (KUDELSKI ANDRE ET AL) 1 September 1992 see column 4, line 58 - line 63 see column 5, line 62 - column 6, line 61 see column 8, line 48 - line 58 see figures 1-4, 8-11	1-14, 36-47
X	WO 96 06504 A (THOMSON CONSUMER ELECTRONICS ; CHANEY JOHN WILLIAM (US)) 29 February 1996 see page 1, line 21 - page 3, line 11 see page 6, line 1 - page 23, line 20 see figures 1-8	1-8, 11-14, 25-29, 40-47
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C.		
<input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. "S" document member of the same patent family		
Date of the actual completion of the international search 12 November 1997	Date of mailing of the international search report 24/11/1997	
Name and mailing address of the ISA European Patent Office, P.B. 5618 Patentlaan 2 NL - 2280 HV Rijswijk Tel: (+31-70) 340-2040, Tx 31 051 report. Fax: (+31-70) 340-3015	Authorized officer Van der Zaal, R	

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/EP 97/02107

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	TASKETT J: "SMART CARDS AS A REPLACEABLE SECURITY ELEMENT FOR TELEVISION DELIVERY ACCESS CONTROL" PROCEEDINGS FROM ELEVEN TECHNICAL SESSIONS OF THE ANNUAL CONVENTION AND EXPOSITION OF THE NATIONAL CABLE TELEVISION ASSOCIATION, SAN FRANCISCO, JUNE 6 - 9, 1993, no. CONVENTION 42, 6 June 1993, RUTKOWSKI K, pages 128-132, XP000410492 see the whole document	1-14, 36-47
X	EP 0 679 029 A (SCIENTIFIC ATLANTA) 25 October 1995 see page 8, line 44 - page 11, line 23 see page 12, line 46 - page 15, line 3 see figures 4,5,7-10 see figures 12,13	15-20, 22,24-49
A	VIGARIE J P: "A DEVICE FOR REAL-TIME MODIFICATION OF ACCESS CONDITIONS IN A D2-MAC/PACKET EUROCRYPT SIGNAL: THE TRANSCONTROLLER" CABLE TV SESSIONS, MONTREUX, JUNE 10 - 15, 1993, no. SYMP. 18, 11 June 1993, POSTES;TELEPHONES ET TELEGRAPHES SUISSES, pages 761-769, XP000379391 see the whole document	15-50

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No.

PCT/EP 97/02107

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5144663 A	01-09-92	AU 599646 B	26-07-90
		AU 7157887 A	22-10-87
		DE 3751410 D	24-08-95
		DE 3751410 T	11-04-96
		EP 0243312 A	28-10-87
		EP 0626793 A	30-11-94
		ES 2076931 T	16-11-95
		JP 2610260 B	14-05-97
		JP 63023488 A	30-01-88
		JP 2520217 B	31-07-96
		JP 5244591 A	21-09-93
WO 9606504 A	29-02-96	AU 3238595 A	22-03-96
		AU 3239495 A	14-03-96
		CA 2196406 A	07-03-96
		CA 2196407 A	29-02-96
		EP 0782807 A	09-07-97
		FI 970677 A	18-02-97
		PL 318647 A	07-07-97
		WO 9607267 A	07-03-96
EP 0679029 A	25-10-95	US 5237610 A	17-08-93
		EP 0683614 A	22-11-95
		AT 144670 T	15-11-96
		AU 650958 B	07-07-94
		AU 1384092 A	01-10-92
		CN 1066950 A,B	09-12-92
		DE 69214698 D	28-11-96
		DE 69214698 T	06-03-97
		EP 0506435 A	30-09-92
		JP 5145923 A	11-06-93

フロントページの続き

(51)Int.Cl.	識別記号	F I	キーワード (参考)
G 0 9 C 1/00	6 6 0	G 0 6 K 19/00	N
H 0 4 H 1/00			Q
H 0 4 L 9/10		H 0 4 L 9/00	6 2 1 A

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(GH, KE, LS, MW, SD, SZ, UG), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU